# Table of Contents


## Chapter 1 Product Overview.....1

A. Introduction ..... 1

B. Contents..... 1

C. **CTIP-01** LED Indications..... 2

## Chapter 2 Your First-Time on CTIP-01 .....3

A. Quick Start Guide..... 3

B. Initial Setting Procedures..... 8

C. Disabling the Mouse Acceleration on the Host Computer and Client Computer..... 14

D. How to Connect your **CTIP-01** ..... 15

I. Connect to the Host Computer ..... 16

II. Connect to the Local Keyboard, Mouse, and Monitor..... 16

III. Connect to the KVM switch..... 17

E. Access your **CTIP-01** and Remote Control the Host Computer ..... 17

## Chapter 3 Advanced Operations .....18

A. How to Login the **CTIP-01** ..... 18

B. Configure your **CTIP-01**..... 19

I. How to Setup the IP Address for your **CTIP-01** ..... 19

II. How to Edit the User Accounts..... 20

III. How to Setup your **CTIP-01** System Identification..... 21

IV. How to Strengthen your **CTIP-01** System Security..... 21

V. How to Setup your **CTIP-01** with the External KVM, External Power Bar, Keyboard Mapping, and USB Keyboard/Mouse Emulation ..... 23

VI. How to Setup Port Numbers ..... 24

VII. How to Lookup your **CTIP-01** System Status..... 24

VIII. How to Setup the SNMP Agent and Configuration ..... 25

IX. How to Setup RADIUS authentication ..... 25

X. How to Setup and Control the External Serial Consoles..... 26

XI. How to Set Date and Time..... 26

XII. How to Update your Firmware ..... 26

XIII. How to Upload Custom Certificate..... 27

XIV. How to Speed up your **CTIP-01** ..... 28

**Chapter 4 File Transfer ..... 29**
A. The File Transfer Screen ..... 29
B. Floppy Mode ..... 29
C. RAM Disk Mode ..... 30
D. CD-ROM Mode ..... 30
E. How to Remotely Booting your Computer ..... 31

**Chapter 5 How to Remotely Control the Host Computer ..... 32**
A. Accessing the VNC Interface ..... 32
I. Web Interface ..... 32
II. Native VNC Client ..... 32
III. SSH Tunnel ..... 33
B. Using the VNC Menu ..... 33
C. How to Use the Bribar ..... 34
D. How to Use the Main Menu ..... 35
E. How to Use the Virtkeys Menu ..... 36
F. How to Use the Video Tuning Menu ..... 37
G. How to Use the Disk Control Menu ..... 38

**Appendices ..... 39**
Appendix A Troubleshooting ..... 39
Appendix B Specifications ..... 42
Appendix C Supported Protocols ..... 43
Appendix D Using Optional Serial Supervisor Module (IPMI supported) with the R-Port of **CTIP-01** ..... 44
Appendix E Using Optional Modem Feature ..... 51
Appendix F The Installation of Optional **CTIP-01** Rack Mounting Bracket: **RACKMT-IP** ..... 55

# Chapter 1 Product Overview

## A. Introduction

**Connect-Tek**'s **CTIP-01** allows network administrators to control and monitor computers or servers from anywhere around the world over the Internet, as well as BIOS level remote control of a target server or servers connected to a KVM switch over a TCP/IP network. The network's administrators can control, reset, and even reboot computers or servers in a server room from a remote location and even watch the entire boot process remotely. The **CTIP-01** offers unique USB capability and the ability to transfer files to the computer or server from a remote location. Remote CD-ROM emulation even allows you to install or update your server's Operating System via an Internet connection. This powerful server administrator tool is ideal for where downtime is not acceptable.

The **CTIP-01** is controlled from any web browser, eliminating the need for proprietary client access software, saving thousands of dollars in per user licensing fees. Security is assured for your sensitive data using several security mechanisms, including Radius authentication, SSH tunneling, etc. The **CTIP-01** is compatible with most existing KVM switches and provides full cross-platform and multiple operating system support.

## B. Contents

This package should contain:

**CTIP-01**

- 1 x **CTIP-01** unit
- 1 x Power Adapter
- 1 x AC Cord for Power Adapter
- 1 x 3-in-1 PS/2 KVM cable
- 1 set of Foot Pads
- 1 x User's Manual

**Required Cables**

- 1 x RS-232 cable (9-pin RS-232 (straight pin-out))
- 1 x Ethernet cable (10/100 Mbits/sec Category 5 or better Ethernet cable)

**Optional Items**

- **CTIP-01** Rack Mounting Bracket, **RACKMT-IP**. A special bracket is available for the rack-mounting **CTIP-01**. It allows rack mounting in two different orientations ---horizontally and vertically, refers to **Appendix F** for more details.
- USB cable ( Five-pin mini-B to standard type-A)

## C. CTIP-01 LED Indications

**Front View of CTIP-01**

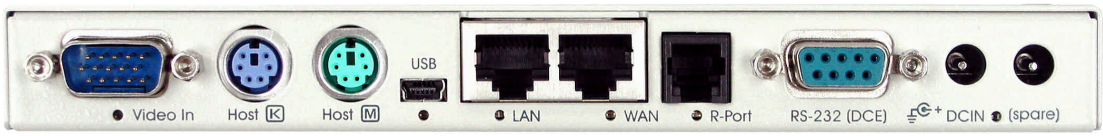
Reset *****LEDs DTE Serial Local K Local M Video (Out)

**LEDs are, from left to right: Power, R- Port, WAN link, LAN link, USB, Video OK*

- **Power**: Indicates one or both of the DC power inputs is providing your system with power.
- **R-Port**: See **Appendix D** for more information about the R-Port.

- **WAN Link / LAN Link**: This is the standard "link light" which is typical for Ethernet equipment. It means the network cable is connected to working Ethernet hub or switch. It lights up with a link connection and blinks with network activity. The LEDs under the Ethernet connectors respond in a similar manner.
- **USB**: This lights up when the USB port is connected to a host and that host has configured the USB port for use. It will blink when USB data is transmitted.
- **Video OK**: This light is lit when a valid VGA signal is received from the host. It is off while in power save mode, if no video is connected or if the host is off.

**Rear View of CTIP-01**




Video (IN) Host K Host M USB LAN WAN R-Port RS-232 (DCE) DC-in Spare

# Chapter 2 Your First-Time on CTIP-01

## A. Quick Start Guide

For this Quick Start Guide, we offer three different easy step-by-step ways, letting you setup this unit very easily and quickly.

**Before doing the initial setting:**

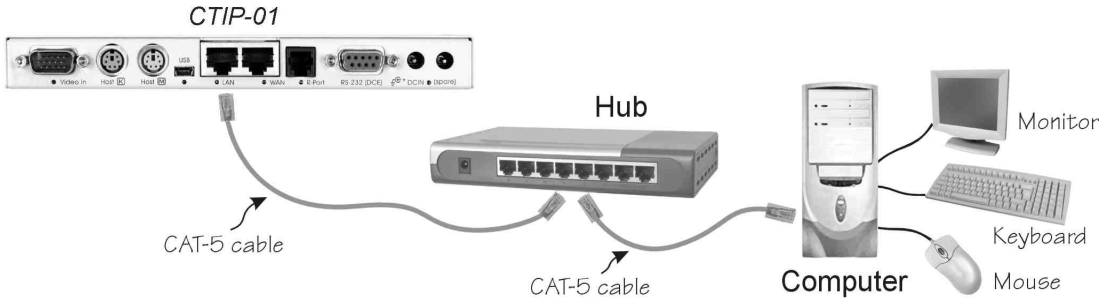
- **Please record your original computer settings such as TCP/IP setting in case you would like to have this computer for other use.**
- **Please make sure the latest Java software downloaded at http://www.java.com.**
- **Please disable mouse acceleration on the host Computer and client computer, refer to more detailed information in Section C of Chapter 2.**

**Hardware Necessary for this Quick Start Guide**

- **A CTIP-01 unit with a power adapter**
- **A hub with a power adapter**
- **A computer with a keyboard, mouse, and monitor**
- **2 CAT-5 cables with RJ-45 connectors**
- **A DB9 RS-232 null modem cable or a DB9 RS-232 straight-through cable**

**1. If you don't have DHCP (Dynamic Host Configuration Protocol)**

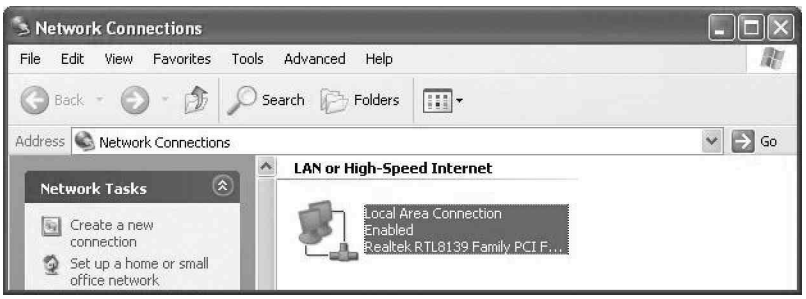
**Step 1**. Connect the CAT-5 cable to the **WAN** port on the rear panel of **CTIP-01**. And, connect the opposite end of the CAT-5 cable to the hub. Another CAT-5 cable connects the hub with the computer.



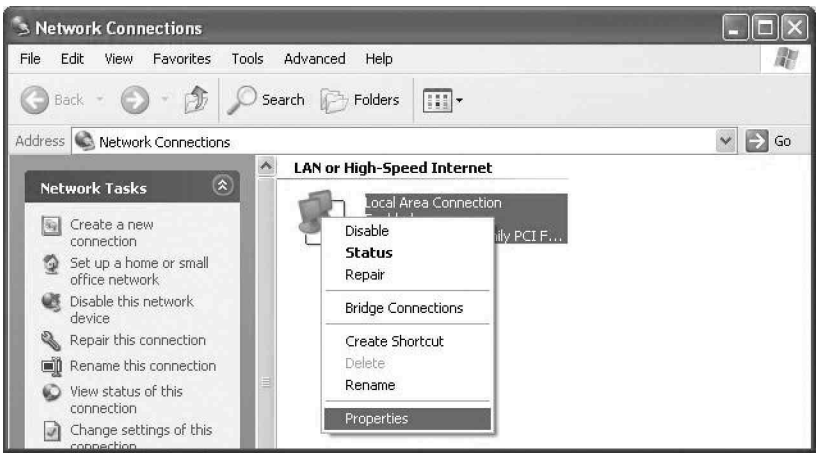

**Step 2**. Set the IP address of a computer connected on the same network as **CTIP-01** to a similar unused address like **192.168.1.124** and the subnet mask of **255.255.255.0**.

**Under Windows XP Environment**

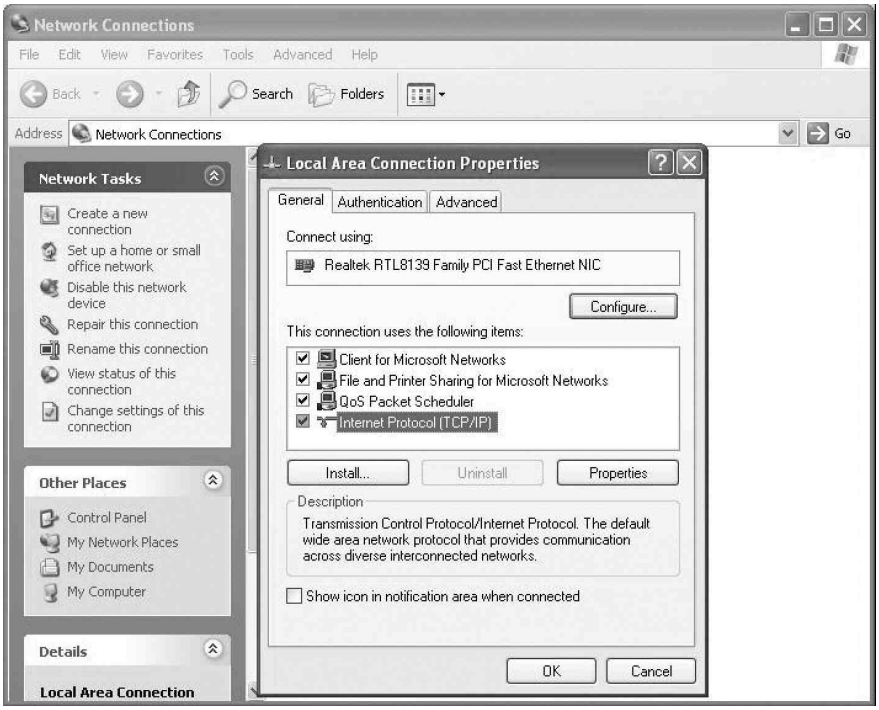
**a**. Click "**Start**", then right click on "**My Network Places**", and then select "**Properties**". You will get the following screen:



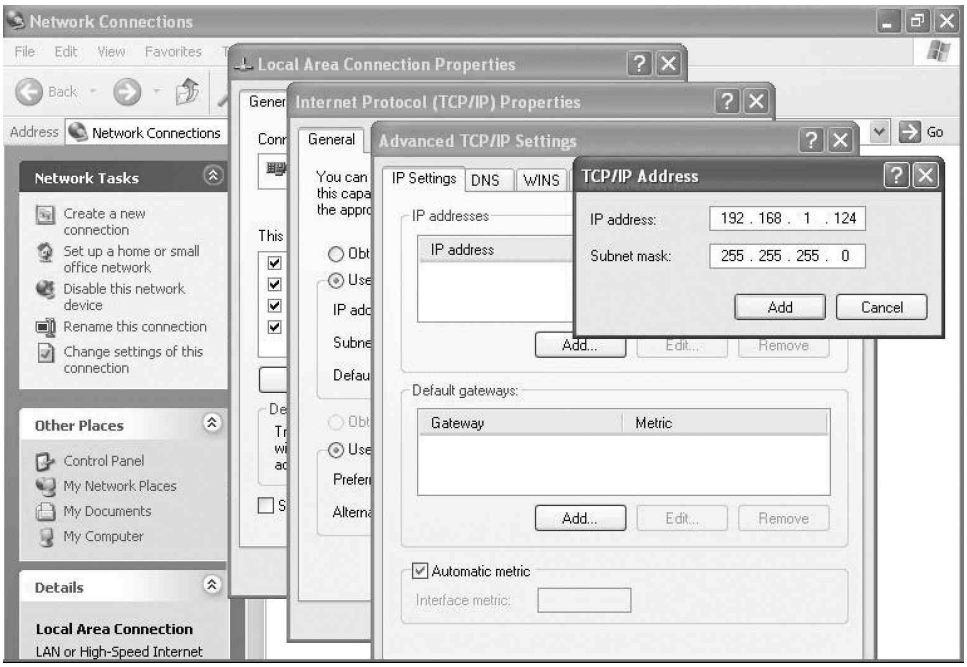
**b**. Right click on "**Local Area Connection**", and select "**Properties**".




**c**. Double click on "**Internet Protocol (TCP/IP)**".



**d**. Click "**Advanced…**", then click "**Add…**" to add up the IP address of "**192.168.1.124**", and the Subnet mask of "**255.255.255.0**".




**Step 3**. From that computer, open a web browser and go to **https://192.168.1.123**. Login using "**admin**" for both username and password.

**Step 4**.Click on the **Admin/Setup** button then **Network configuration (IP address, netmask, gateway)**. From here you can set the IP address as needed.

**2. If you have DHCP (Dynamic Host Configuration Protocol)**

**Step 1**. Please have your **MAC address**. You can find it on a white sticker on the bottom of the **CTIP-01**. Here is an example, **00-0E-C5-00-08-1A**.

**Step 2**. Power on the **CTIP-01** and connected to the network via **WAN** port on the rear panel. The **DHCP** will automatically assign an IP address to the **CTIP-01.**

**Step 3**. Access the **DHCP log** from your **file server**. A simple **DHCP log** looks similar to the following:

**DHCP Client Log**

DHCP Client Log View your LAN client's information that are currently linked to the Broadband router's DHCP server.

Numbers of DHCP Clients: 3

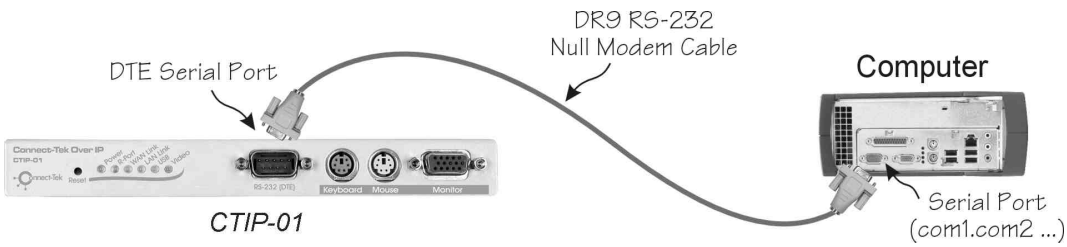
```
ip=192.168.22.3   mac=00-03-93-D1-D7-18   name=stpcpm18
ip=192.168.22.4   mac=00-0E-C5-00-0A-FC
ip=192.168.22.5   mac=00-00-39-03-56-D6   name=STPCMOBILE01
```

**Step 4**. From the above **DHCP** log, you can easily find the **DHCP** assigned an IP to the **CTIP-01, 192.168.22.4**. Once you have located this IP address, do NOT power off the **CTIP-01** or your **DHCP** server since it might lease a different IP address.

**Step 5**. Simply open a web browser and type **https://192.168.22.4** to access your **CTIP-01**. Login using "**admin**" for both username and password.

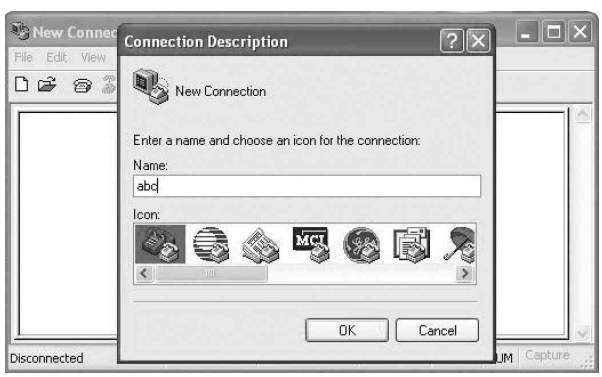
**3. Using the HyperTerminal via Serial Port**

**Step 1**. Connect the **DB9 RS-232 Null Modem cable** (optional) to the **DTE** serial port on the rear panel of **CTIP-01**. And, connect the opposite end of the cable to the serial port (**COM1, COM2**…) of your computer.



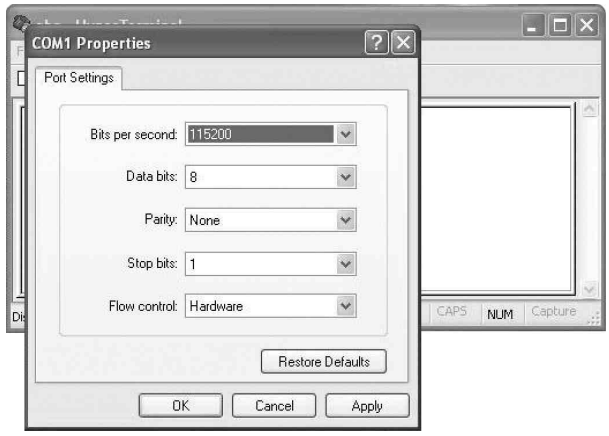

**Step 2**. From your computer, select "**HyperTerminal**" as following.

**Step 3**. If you never setup your **HyperTerminal** before, it will ask you to input your phone area code, please feel free to do so, and then click "**OK**", you will get the following screen. Please type any name you prefer, for example, "**abc**".

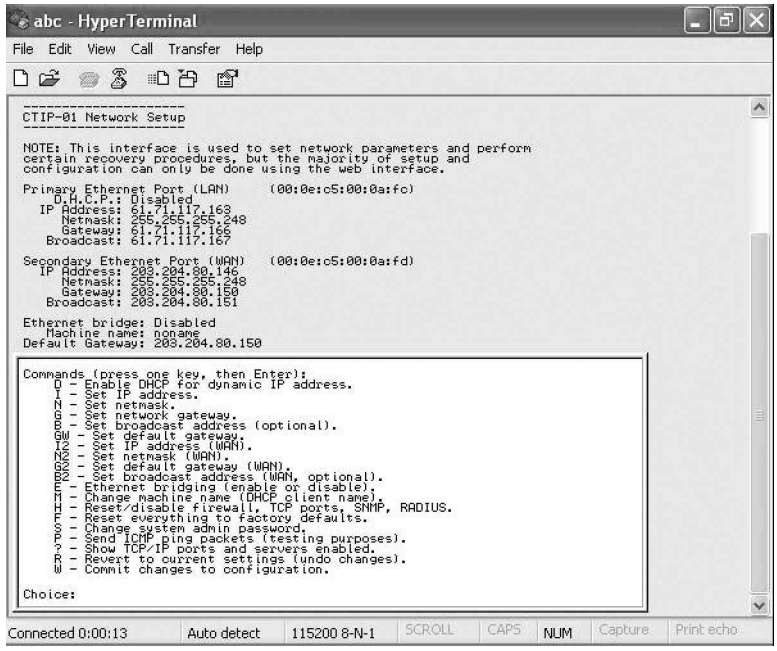


**Step 4**. Choose the proper serial port you connect.

**Step 5**. Change "**Bits per second**" to **115200**.




**Step 6**. Press "**Enter**", you will get the following screen.


abc - HyperTerminal
File Edit View Call Transfer Help
CTIP-01 Network Setup
NOTE: This interface is used to set network parameters and perform certain recovery procedures, but the majority of setup and configuration can only be done using the web interface.
Primary Ethernet Port (LAN) (00:0e:c5:00:0a:fc)
D.H.C.P.: Disabled
IP Address: 61.71.117.163
Netmask: 255.255.255.248
Gateway: 61.71.117.166
Broadcast: 61.71.117.167
Secondary Ethernet Port (WAN) (00:0e:c5:00:0a:fd)
IP Address: 203.204.80.146
Netmask: 255.255.255.248
Gateway: 203.204.80.150
Broadcast: 203.204.80.151
Ethernet bridge: Disabled
Machine name: noname
Default Gateway: 203.204.80.150
Commands (press one key, then Enter):
0 - Enable DHCP for dynamic IP address.
I - Set IP address.
N - Set netmask.
G - Set network gateway.
B - Set broadcast address (optional).
GW - Set default gateway.
I2 - Set IP address (WAN).
N2 - Set netmask (WAN).
G2 - Set default gateway (WAN).
B2 - Set broadcast address (WAN, optional).
E - Ethernet bridging (enable or disable).
M - Change machine name (DHCP client name).
H - Reset/disable firewall, TCP ports, SNMP, RADIUS.
F - Reset everything to factory defaults.
S - Change system admin password.
P - Send ICMP ping packets (testing purposes).
? - Show TCP/IP ports and servers enabled.
R - Revert to current settings (undo changes).
W - Commit changes to configuration.
Choice:
Connected 0:00:13
Auto detect
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

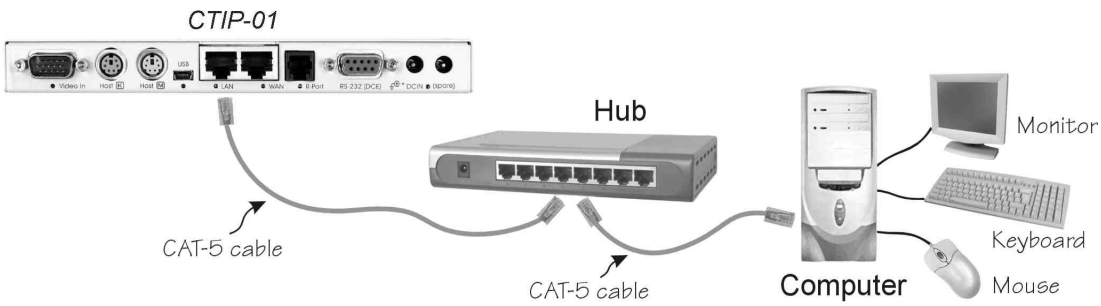
**Step 7**. Follow the instructions on the screen. For example, simply type "**I**" for setting your IP, type "**M**" for changing the machine name, and so on. Here is a reminder for you, please type "**W**" after you made any change.

## B. Initial Setting Procedures

Before installing your **CTIP-01**, please refer to the "**Contents**" section of **Chapter 1** to ensure that you have all of the necessary items for the following proper installation.
Just choose either one method of assigning an IP address. There are **3 available methods** of assigning an IP address to the **CTIP-01**:

### 1. DHCP

**Step 1**: Connect your network to the **LAN** Port of **CTIP-01**. The first time the unit is booted, it will perform **DHCP** lease request to get an IP address. Therefore, you'd better connect it to the network before turning it on.




**Step 2**: Please have your **MAC address**. You can find it on a white sticker on the bottom of the **CTIP-01**. Here is an example, **00-0E-C5-00-08-1A**.

**Step 3**: Power on the **CTIP-01** and connected to the network via **WAN** port on the rear panel. The **DHCP** will automatically assign an IP address to the **CTIP-01.**

**Step 4**: Access the **DHCP log** from your **file server**. A simple **DHCP log** looks similar to the following:

**DHCP Client Log**

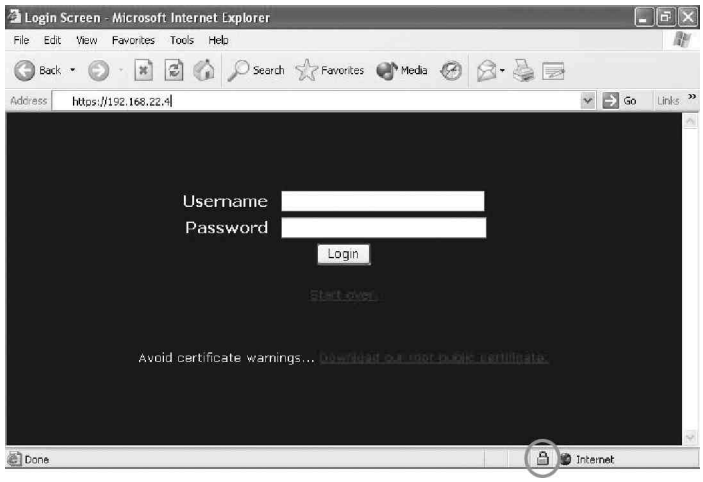
DHCP Client Log View your LAN client's information that are currently linked to the Broadband router's DHCP server.

Numbers of DHCP Clients: 3

```
ip=192.168.22.3   mac=00-03-93-D1-D7-18   name=stpcpm18
ip=192.168.22.4   mac=00-0E-C5-00-0A-FC
ip=192.168.22.5   mac=00-00-39-03-56-D6   name=STPCMOBILE01
```

**Step 5**: From the above **DHCP** log, you can easily find the **DHCP** assigned an IP to the **CTIP-01, 192.168.22.4**. Once you have located this IP address, do NOT power off the **CTIP-01** or your **DHCP server** since it might lease a different IP address.

**Step 6**: Simply open a web browser and type **https://192.168.22.4** to access your **CTIP-01**. Login by using "**admin**" for both username and password. **NOTE**: **Please remember to type "s" after http**. And, you will see a **Lock** on the lower right corner of your screen. That means all of your information is under the protection of **128-bit SSL Encryption**.

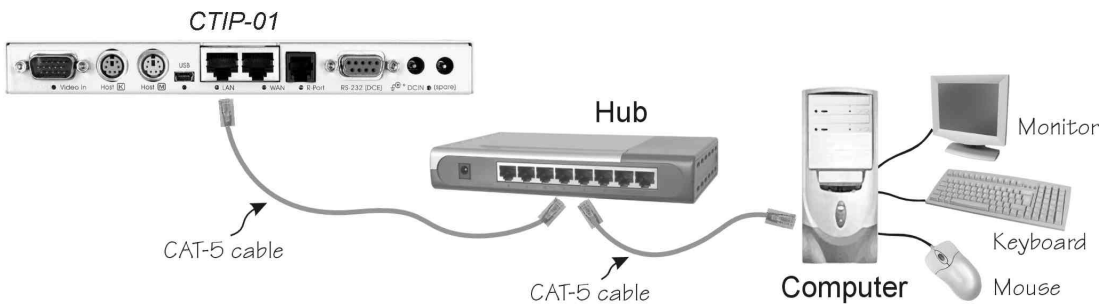



**2. Fixed IP address**

Connect your network to the **WAN** Port of **CTIP-01**. This following are the default values for the **WAN** port of **CTIP-01**:

IP Address: **192.168.1.123**
Subnet Mask: **255.255.255.0**
Default Gateway: **192.168.1.254**
Broadcast: **192.168.1.255**

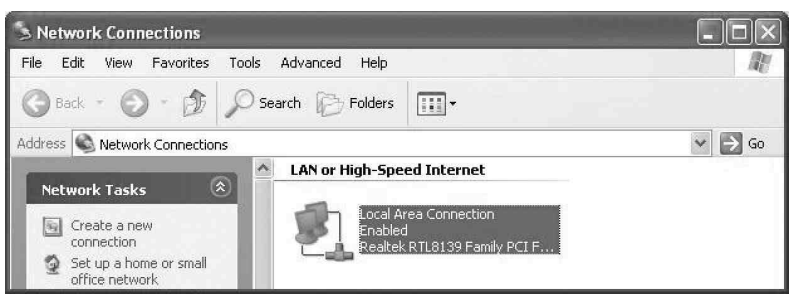
**Step 1**: Connect the CAT-5 cable to the **WAN** port on the rear panel of **CTIP-01**. And, connect the opposite end of the CAT-5 cable to the hub. Another CAT-5 cable connects the hub with the computer.




**Step 2**: Set the IP address of a computer connected on the same network as **CTIP-01** to a similar unused address like **192.168.1.124** and the subnet mask of **255.255.255.0**.

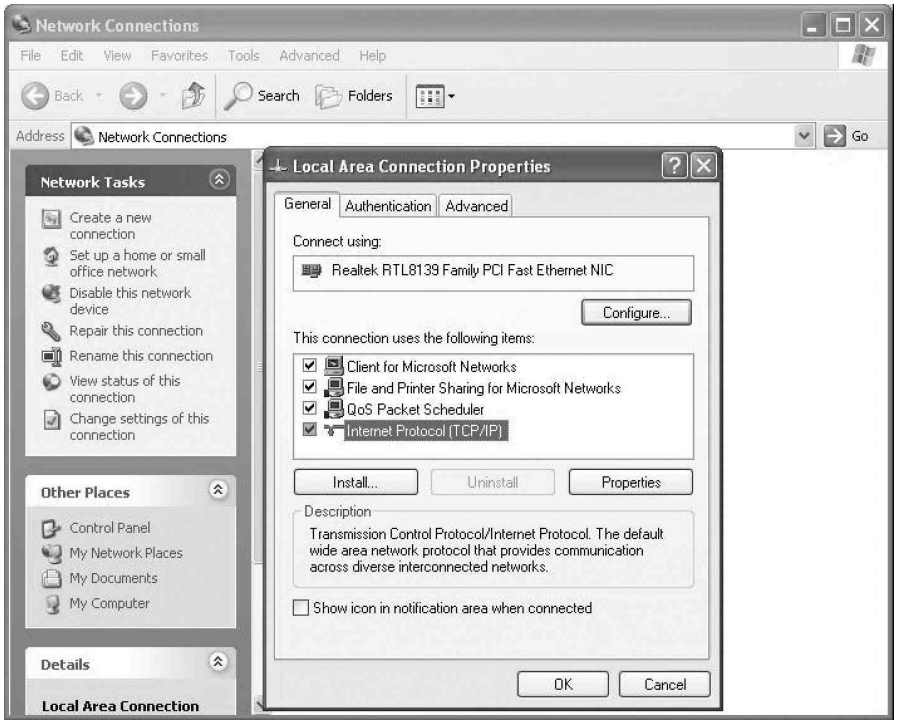
**Under Windows XP environment**

- Click "**Start**", then right click on "**My Network Places**", and select "**Properties**". You will get the following screen:

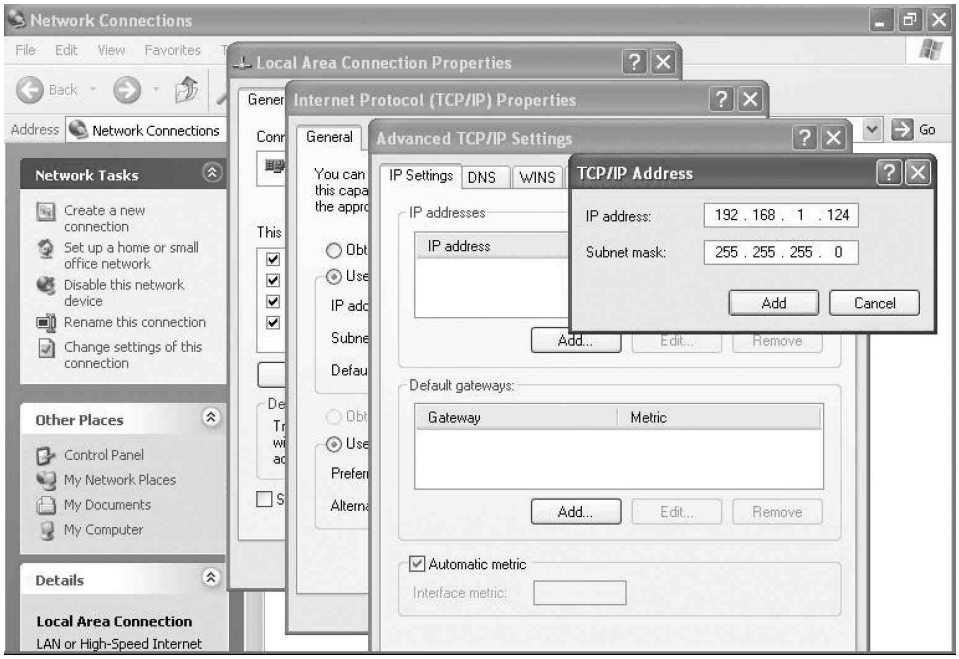


- Right click on "**Local Area Connection**", and select "**Properties**".

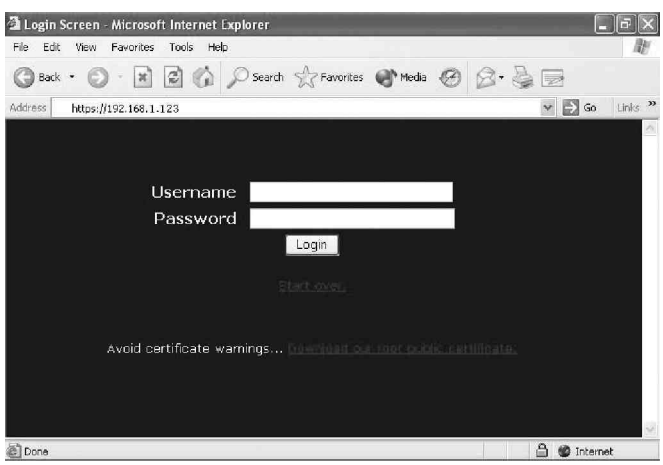
- Double click on "**Internet Protocol (TCP/IP)**".



- Click "**Advanced…**", then click "**Add…**" to add up the IP address of "**192.168.1.124**", and the Subnet mask of "**255.255.255.0**".

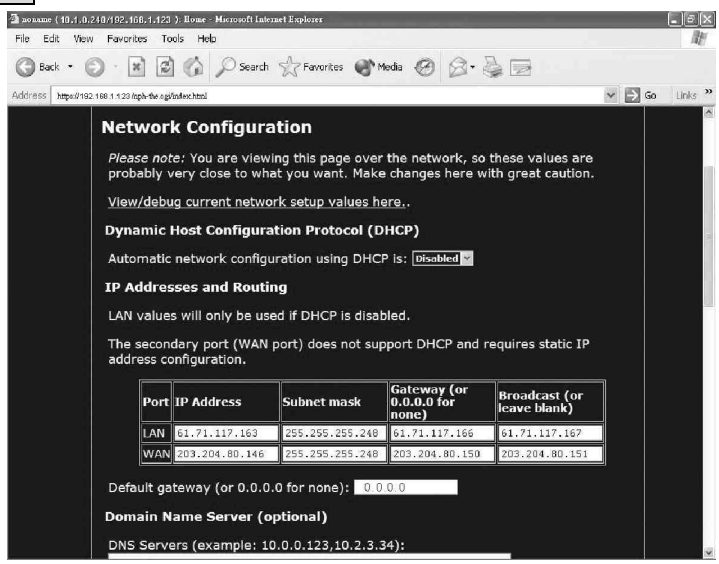



**Step 3**: From that computer, open a web browser and go to **https://192.168.1.123**. Login by using "**admin**" for both of username and password.



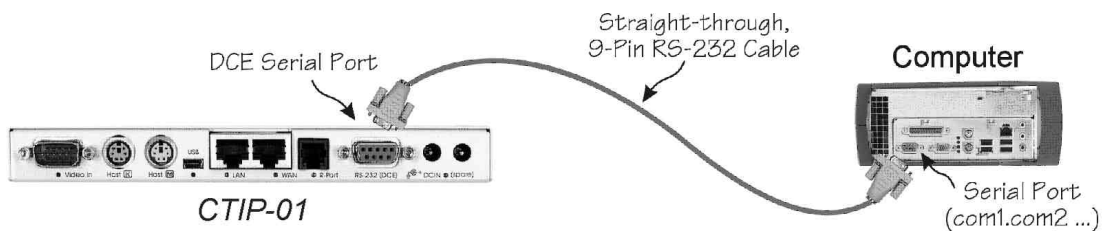
**Step 4**: Click on the **Admin/Setup** button then **Network configuration (IP address, netmask, gateway)**.

**Step 5**: From here you can set the IP address as needed, as soon as you set your IP addresses up, simply press **Commit**.


Network Configuration
Please note: You are viewing this page over the network, so these values are probably very close to what you want. Make changes here with great caution.
View/debug current network setup values here..
Dynamic Host Configuration Protocol (DHCP)
Automatic network configuration using DHCP is: Disabled
IP Addresses and Routing
LAN values will only be used if DHCP is disabled.
The secondary port (WAN port) does not support DHCP and requires static IP address configuration.
Port
IP Address
Subnet mask
Gateway (or 0.0.0.0 for none)
Broadcast (or leave blank)
LAN
61.71.117.163
255.255.255.248
61.71.117.166
61.71.117.167
WAN
203.204.80.146
255.255.255.248
203.204.80.150
203.204.80.151
Default gateway (or 0.0.0.0 for none): 0.0.0.0
Domain Name Server (optional)
DNS Servers (example: 10.0.0.123,10.2.3.34):

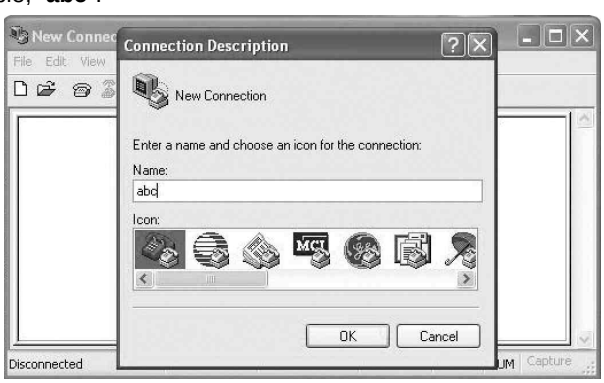
### 3. Serial Port (DCE)

Connect the rear-panel RS-232 serial port (DCE) to a computer that can be used temporarily for setup and control. This serial port connection is not required once the unit is initially setup and configured. It is an 115,200 BPS (8N1) connection. A straight-through, 9-pin RS-232 cable is used, **not** a null-modem cable.



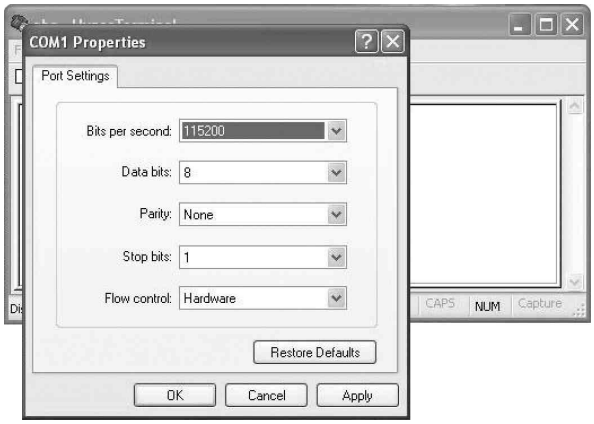
**Step 1**: From your computer, select "**HyperTerminal**" as following.

**Step 2**: If you never setup your **HyperTerminal** before, it will ask you to input your phone area code, please feel free to do so, and then click "**OK**", you will get the following screen. Please type any name you prefer, for example, "**abc**".

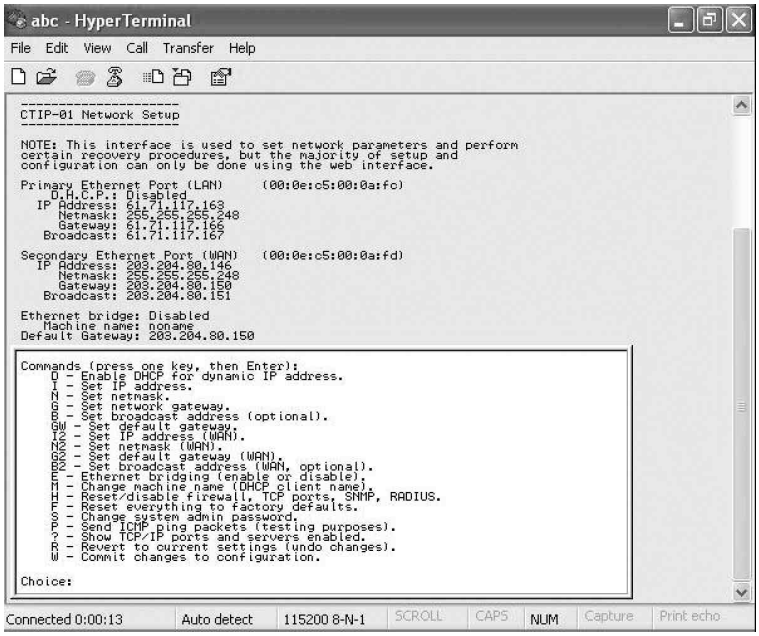



**Step 3**: Choose the proper serial port you connect.

**Step 4**: Change "**Bits per second**" to **115200**.




**Step 5**: Press "**Enter**", you will get the following screen.


abc - HyperTerminal
File Edit View Call Transfer Help
CTIP-01 Network Setup
NOTE: This interface is used to set network parameters and perform certain recovery procedures, but the majority of setup and configuration can only be done using the web interface.
Primary Ethernet Port (LAN) (00:0e:c5:00:0a:fc)
D.H.C.P.: Disabled
IP Address: 61.71.117.163
Netmask: 255.255.255.248
Gateway: 61.71.117.166
Broadcast: 61.71.117.167
Secondary Ethernet Port (WAN) (00:0e:c5:00:0a:fd)
IP Address: 203.204.80.146
Netmask: 255.255.255.248
Gateway: 203.204.80.150
Broadcast: 203.204.80.151
Ethernet bridge: Disabled
Machine name: noname
Default Gateway: 203.204.80.150
Commands (press one key, then Enter):
D - Enable DHCP for dynamic IP address.
I - Set IP address.
N - Set netmask.
G - Set network gateway.
B - Set broadcast address (optional).
GW - Set default gateway.
I2 - Set IP address (WAN).
N2 - Set netmask (WAN).
G2 - Set default gateway (WAN).
B2 - Set broadcast address (WAN, optional).
E - Ethernet bridging (enable or disable).
M - Change machine name (DHCP client name).
H - Reset/disable firewall, TCP ports, SNMP, RADIUS.
F - Reset everything to factory defaults.
S - Change system admin password.
P - Send ICMP ping packets (testing purposes).
? - Show TCP/IP ports and servers enabled.
R - Revert to current settings (undo changes).
W - Commit changes to configuration.
Choice:
Connected 0:00:13
Auto detect
115200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

**Step 6**: Follow the instructions on the screen. For setting up your IPs, you have to key in "IP Address", "Netmask", and "Network Gateway" for both of the **LAN** port and **WAN** port by typing

- "**I**": key in your IP address for the **LAN** port of **CTIP-01**.
- "**N**": key in your Netmask for the **LAN** port of **CTIP-01**.
- "**G**": key in your Network Gateway for the **LAN** port of **CTIP-01**.
- "**I2**": key in your IP address for the **WAN** port of **CTIP-01**.
- "**N2**": key in your Netmask for the **WAN** port of **CTIP-01**.
- "**G2**": key in your Network Gateway for the **WAN** port of **CTIP-01**.

Here is a reminder, **please type "W" after you made any change**.

## C. Disabling Mouse Acceleration on the Host Computer and Client Computer

As soon as you finish the instructions of one of the above three methods, **please do remember to disable**

**mouse acceleration on BOTH of the host computer AND the client computer to avoid the mouse not lining up on the VNC screen.**

Many operating systems offer a feature called mouse acceleration that allows the user to adjust the responsiveness of the cursor on the screen to physical movements of the mouse. While this is usually a beneficial interface enhancement, it can interfere with the operation of the **CTIP-01** and should be disabled on BOTH the host computer AND the client computer before a remote session is attempted. Follow the instructions below to disable mouse acceleration for the operating system installed on the host computer as well as the client computer.

**Windows 98 / 2000**

1. From the **Control Panel**, click on **Mouse**.
2. From **Mouse Properties**, click on **Mouse tab**.
3. Make sure the **Pointer speed bar** is centered and **Acceleration** is set to **None**.

**Windows XP and Windows Server 2003**

1. Go to "**Pointer Options**" and turn off "**Enhance Pointer Precision**".
2. Make sure that the **Pointer speed bar** is centered.

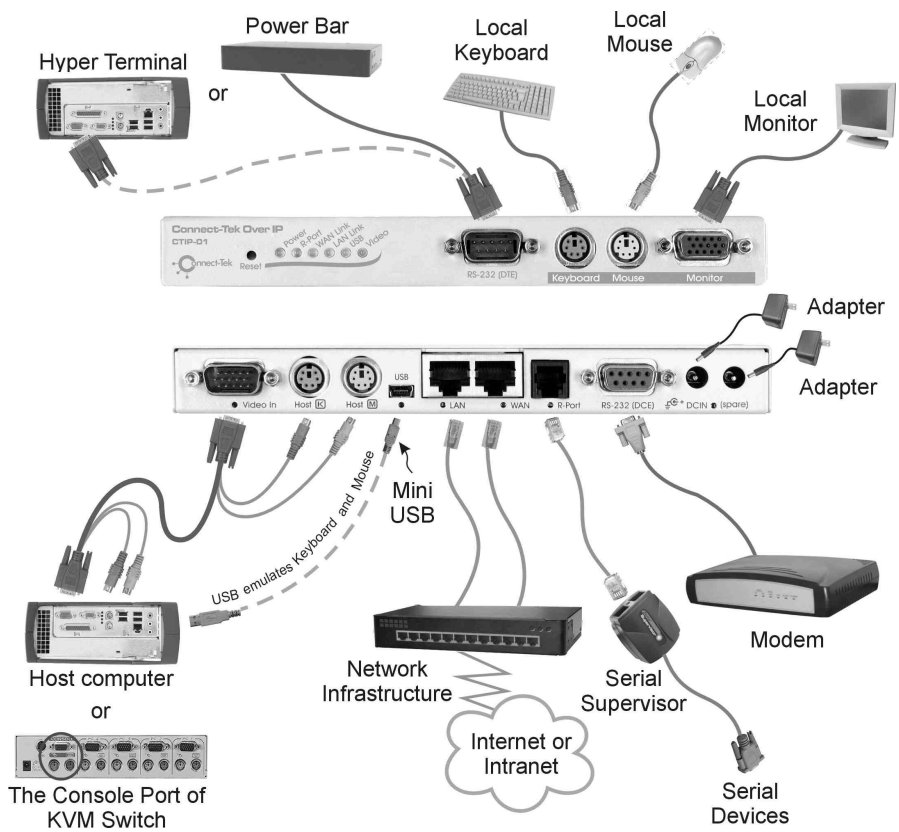
**Linux, Unix, and X-Windows**

Add this command to your xinitrc, xession or other startup script: **xset m 0/0 0**

**Sun Solaris**

Add this command to your xinitrc, xession or other startup script: **xset m 1/1 0**

## D. How to Connect your CTIP-01



**Note:** All of the above devices are not included except the **CTIP-01**, one adapter, and one 3-in-1 KVM PS/2 cable. And, the Power Bar, Mini-USB to USB cable, Serial Supervisor, and Modem device are optional.

## I. Connect to the Host Computer

**a. If your host computer uses the PS/2 keyboard and mouse, please follow the instructions below:**

1. Turn off your host computer and leave your **CTIP-01** powered down. If you purchase **CTIP-01** Rack Mounting Bracket (optional), please install it with **CTIP-01** on your rack or cabinet.
2. Use **3-in-1 KVM PS/2 cable** (included) to connect the **Host Keyboard**, **Host Mouse, Video (IN)** of **CTIP-01** with the PS/2 keyboard port, PS/2 mouse port, video port of your host computer.
3. Use the **CAT-5 Ethernet cable** to connect the **LAN** port of **CTIP-01** with a network data jack such as the hub, switch, router, pre-wired wall jack, and so on.
4. (Optional) If you would like to connect the **WAN** port of **CTIP-01** as well, please apply step 3 on the **WAN** port.
5. Connect the **power cord** (included) into an appropriate electrical outlet; plug the opposite end of the power cord into the **AC/DC adapter**, then plug the power connector into the **DC-in** port of **CTIP-01**. The LED underneath the power connectors will be solid green when the **CTIP-01** is powered.
6. (Optional) If you would like to add power redundancy to the **CTIP-01**, simply connect the **optional second AC/DC adapter** to the **Spare** port of **CTIP-01**. This provides a load-balancing feature between the two power sources and allows the **CTIP-01** to function if one adapter fails.
7. Turn on your host computer.

**b. If your host computer uses the USB keyboard and mouse, please follow the instructions below:**

1. Turn off your host computer and leave your **CTIP-01** powered down. If you purchase **CTIP-01** Rack Mounting Bracket (optional), please install it with **CTIP-01** on your rack or cabinet. **NOTE**: The **CTIP-01** is convection-cooled. Ensure the vents on both sides are unobstructed.
2. Use the **HDB-15 VGA cable** to connect the **Video (IN)** port of **CTIP-01** with the video port of your host computer.
3. Use the **USB Type A to 5-pin mini-B cable** (not included) to connect the **mini USB** port of **CTIP-01** with an available USB port on the host computer. This **mini USB** can emulate the keyboard and mouse. In the event that you do not have enough integrated USB ports on the host computer to directly connect the keyboard, mouse, and **CTIP-01**, you may use a high-quality USB hub on one of the computer's USB ports to make all of the connections.
4. Use the **CAT-5 Ethernet cable** to connect the **LAN** port of **CTIP-01** with a network data jack such as the hub, switch, router, pre-wired wall jack, and so on.
5. (Optional) If you would like to connect the **WAN** port of **CTIP-01** as well, please apply step 3 on the **WAN** port.
6. Connect the **power cord** (included) into an appropriate electrical outlet; plug the opposite end of the power cord into the **AC/DC power adapter**, then plug the power connector into the **DC-in** port of **CTIP-01**. The LED underneath the power connectors will be solid green when the **CTIP-01** is powered.
7. (Optional) if you would like to add power redundancy to the **CTIP-01**, simply connect the **optional second AC/DC power adapter** to the **Spare** port of **CTIP-01**. This provides a load-balancing feature between the two power sources and allows the **CTIP-01** to function if one adapter fails.
8. Turn on your host computer.

## II. Connect to the Local Keyboard, Mouse, and Monitor

The **CTIP-01** offers the **Local Keyboard** Port, **Local Mouse** Port, and **Video (Out)** (local monitor) Port, allowing the user to connect a keyboard, mouse, and a monitor for maintenance and monitoring locally. This allows a user to physically use the host computer as through the **CTIP-01** were transparent.

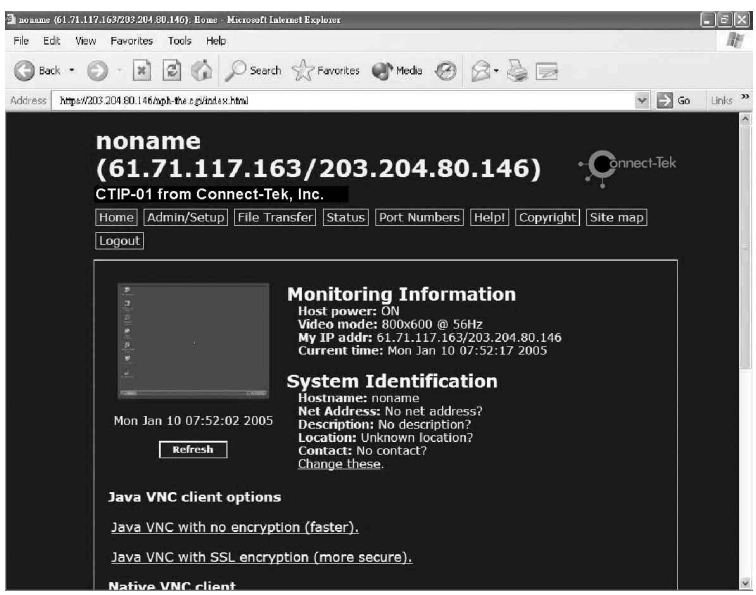
### III. Connect to the KVM Switch

If needed, the **CTIP-01** can be run through a typical KVM switch like any other computer. Using a KVM cable, you can connect the **Host Keyboard** Port, **Host Mouse** Port, and **Video (In)** Port of **CTIP-01** with the "**console**" connectors on a KVM switch. The steps are shown as following:

1. Connect the **Host Keyboard** Port of **CTIP-01** to the keyboard port of the **console** on the KVM switch.
2. Connect the **Host Mouse** Port of **CTIP-01** to the mouse port of the **console** on the KVM switch.
3. Connect the **Video (In)** Port of **CTIP-01** to the video port of the **console** on the KVM switch.
4. Use the **CAT-5 Ethernet cable** to connect the **LAN** port of **CTIP-01** with a network data jack such as the hub, switch, router, pre-wired wall jack, and so on.
5. (Optional) If you would like to connect the **WAN** port of **CTIP-01** as well, please apply step 3 on the **WAN** port.
6. Connect the **power cord** (included) into an appropriate electrical outlet; plug the opposite end of the power cord into the **AC/DC power adapter**, then plug the power connector into the **DC-in** port of **CTIP-01**. The LED underneath the power connectors will be solid green when the **CTIP-01** is powered.
7. (Optional) if you would like to add power redundancy to the **CTIP-01**, simply connect the **optional second AC/DC power adapter** to the **Spare** port of **CTIP-01**. This provides a load-balancing feature between the two power sources and allows the **CTIP-01** to function if one adapter fails.
8. Power on the **CTIP-01** and KVM switch.

## E. Access your CTIP-01 and Remote Control the Host Computer

As soon as you finish the above initial settings and connections, congratulations! You are ready to enjoy remote control the host computer from any corner around the whole world!
Simply open up the web browser and type the IP you setup in the initial settings, and then type the right username and password. That's it! You're ready to access your **CTIP-01**!
As you login the **CTIP-01** with the right username and password, you will get the following screen:




Please simply double click on the small square window in the middle of the screen. You'll get the VNC screen.( **You may need to upgrade or download your Java support in your browser before using the VNC screen to remote control the host computer**; however, most modern browsers come with a version of Java that is compatible with this application.) That is, you will see the screen of the host computer. Now, you can fully control the host computer *remotely* like you are present at the host computer location physically, sitting in front of the host computer! Likewise, if you would like to log out your **CTIP-01**, please simply click on the icon of "Logout" on the top of screen!

# Chapter 3 Advanced Operations

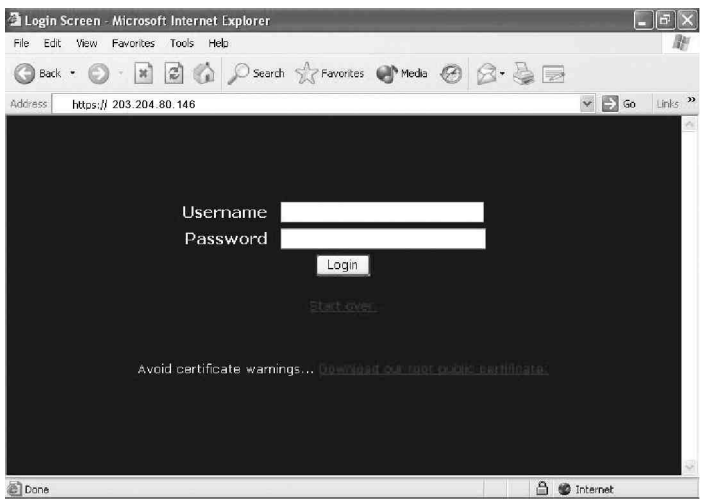
The Web interface is the most intuitive way to configure the **CTIP-01**. It also offers a Java-based VNC client that you can use to control the host computer from a remote location. The **CTIP-01** supports any industry-standard HTML Web browser. You can access the Web interface by opening your Web browser and entering the IP address of the **CTIP-01** you wish to access/configure. The IP address will be either

**a)** The address assigned for the **LAN** port by your **DHCP server** as identified in the previous section.
**or**
**b)** **192.168.1.123** for the **WAN** port if your network uses static IP addressing.

## A. How to Login the CTIP-01

**Step 1: The Login Screen**

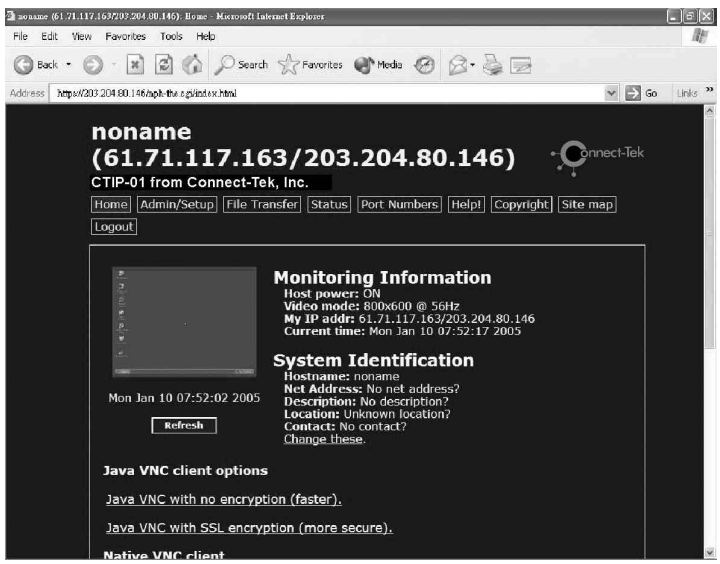
Before you can access the Web configuration interface, you must enter a user name and password. The default username and password as shipped from the factory is username **admin** with a password of **admin**.




**NOTE:** Before the login screen appears, your Web browser may display a warning about an invalid security certificate. This does not affect the security of your data in any way. Whenever you are prompted about a certificate security problem by your browser or the Java VNC client, always choose the option to continue.

**Step 2: The Home Screen**

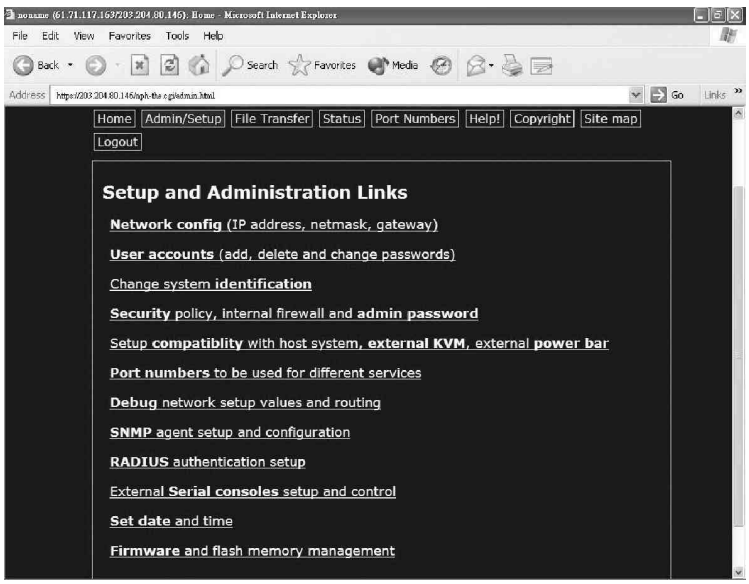
The Home screen serves two functions. First, it is a place to check the status of the **CTIP-01**, view essential system information, and capture screen shots from the host computer. Second, it is where you can start the integrated Java VNC client to interact with the host computer by clicking on the large screen shot or choosing one of the VNC client links.



## B. Configuring your CTIP-01

**The Admin/Setup Screen**

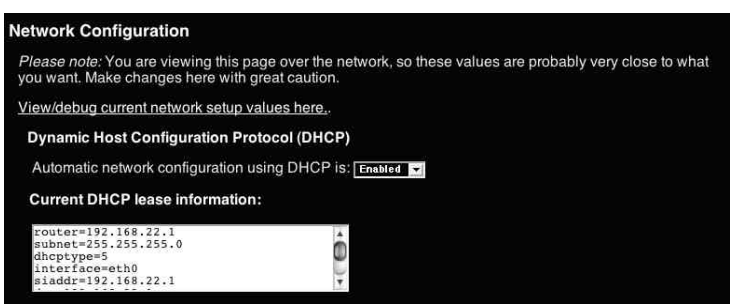
This is the menu that will allow you to access all the features you will need to perform an initial configuration of the **CTIP-01**. Each of the options is explained as following:




## I. How to Setup the IP Address for your CTIP-01

As you get the Admin/Setup screen, please click on **Network Configuration (IP address. Netmask, etc).**

**Dynamic Host Configuration Protocol (DHCP)**
Automatic network configuration using DHCP is: **Enabled/Disabled.**
This feature applies only to the **LAN** port on the rear panel, and is enabled by default. When enabled, the unit will automatically configure itself with an IP address when a **DHCP server** is present. When disabled, the **LAN** port will use the values assigned to it on the **IP Addresses and Routing** table below.

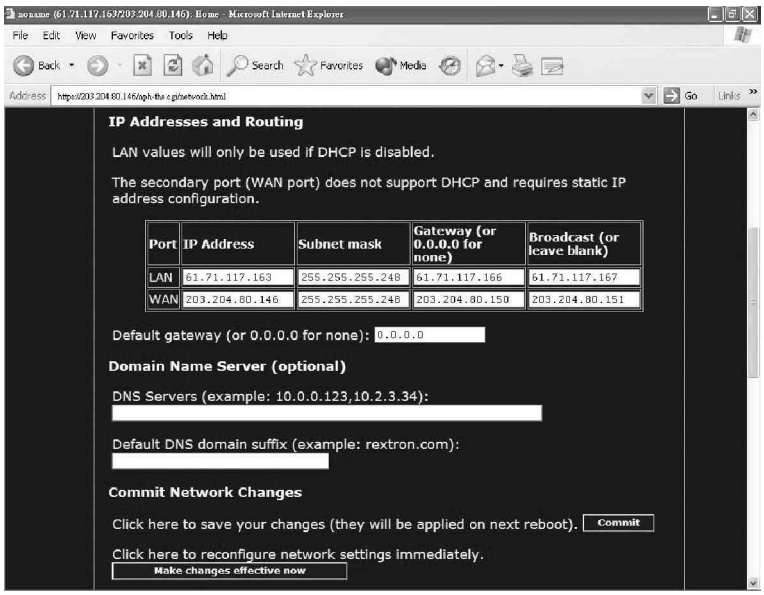

Network Configuration
Please note: You are viewing this page over the network, so these values are probably very close to what you want. Make changes here with great caution.
View/debug current network setup values here.
Dynamic Host Configuration Protocol (DHCP)
Automatic network configuration using DHCP is: Enabled
Current DHCP lease information:
router=192.168.22.1
subnet=255.255.255.0
dhcptype=5
interface=eth0
siaddr=192.168.22.1

**Current DHCP Lease Information**

This box provides detailed information about the IP lease that the unit has obtained from the **DHCP server**.

**IP Addresses and Routing**

This table allows you to assign IP information for the **LAN** and **WAN** ports separately. If you are using DHCP, the values for the **LAN** port will be filled in automatically and any changes made will not affect the setup. If **Ethernet Bridging** is enabled (see below) the **WAN** port will use the same settings as the **LAN** port, and any changes will not affect the setup for that port. Adjusting the setting for the **WAN** port allows you have greater control over how the **CTIP-01** is configured for access from outside the local network, particularly if a firewall or proxy is in use.




**Domain Name Server (optional)**

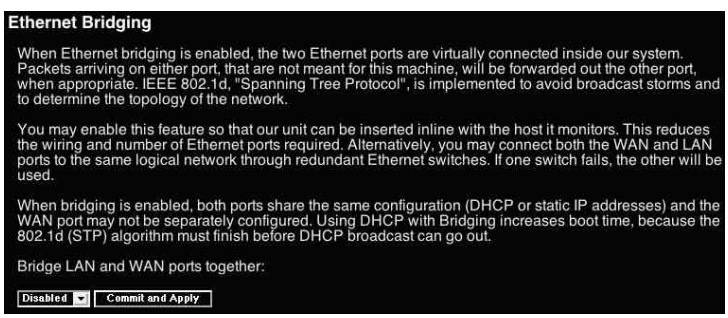
This section allows you to specify DNS servers and the default DNS domain suffix in use on the network. If DHCP is enabled, some of these values may be supplied automatically.

**Commit Network Changes**

Clicking the **Commit** button applies any changes made on the page to the configuration, but leaves the old settings active until the next time the unit restarts. Clicking **Make changes effective now** applies the changes and restarts the **CTIP-01** so the new settings take effect immediately.

**Ethernet Bridging**

When Ethernet bridging is enabled, the two Ethernet ports are virtually connected inside the **CTIP-01**.

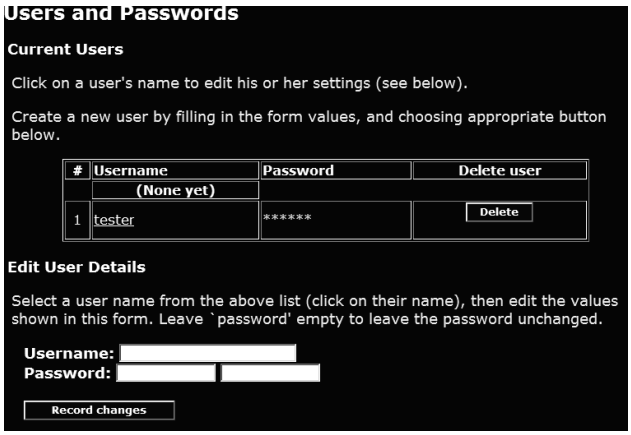

Ethernet Bridging
When Ethernet bridging is enabled, the two Ethernet ports are virtually connected inside our system. Packets arriving on either port, that are not meant for this machine, will be forwarded out the other port, when appropriate. IEEE 802.1d, "Spanning Tree Protocol", is implemented to avoid broadcast storms and to determine the topology of the network.
You may enable this feature so that our unit can be inserted inline with the host it monitors. This reduces the wiring and number of Ethernet ports required. Alternatively, you may connect both the WAN and LAN ports to the same logical network through redundant Ethernet switches. If one switch fails, the other will be used.
When bridging is enabled, both ports share the same configuration (DHCP or static IP addresses) and the WAN port may not be separately configured. Using DHCP with Bridging increases boot time, because the 802.1d (STP) algorithm must finish before DHCP broadcast can go out.
Bridge LAN and WAN ports together:
Disabled
Commit and Apply

1. You may enable this feature so that the module can be inserted inline with the host it monitors. This reduces the wiring and number of Ethernet ports required.
2. Alternatively, you may connect both the **WAN** and **LAN** ports to the same logical network through redundant Ethernet switches. If one switch fails, the other will be used.
3. When bridging is enabled, both ports share the same configuration (DHCP or static IP addresses) and the **WAN** port may not be separately configured.
4. To change this setting, select either Enabled or Disabled from the drop-down menu and click Commit and Apply.

## II. How to Edit the User Accounts

As you get the Admin/Setup screen, please click on **User accounts (add, delete and change passwords).**

This menu will allow you to add accounts other than **admin** to the system. These accounts will not have the authority to change settings, but can access the Web interface and log in the VNC console. Selecting **Delete** permanently removes the user from the system. If you enter values for a user that does not already exist under **Edit User Details**, the system will create that user for you when you click **Record changes**. If the user already exists, you will change the password for that user.


Users and Passwords
Current Users
Click on a user's name to edit his or her settings (see below).
Create a new user by filling in the form values, and choosing appropriate button below.
# Username Password Delete user
(None yet)
1 tester ****** Delete
Edit User Details
Select a user name from the above list (click on their name), then edit the values shown in this form. Leave `password' empty to leave the password unchanged.
Username:
Password:
Record changes

## III. How to Setup your CTIP-01 System Identification

As you get the Admin/Setup screen, please click on **Change system identification.**

The administrator can define the following details:
- machine name
- location
- contact name
- network address
- description

These details are useful for the DHCP servers, SNMP agents, and VNC clients. While these values do not affect the operation of the unit, they make it easier to manage on the network.

## IV. How to Strengthen your CTIP-01 System Security

As you get the Admin/Setup screen, please click on **Security policy, internal firewall and admin password.**

Security Profile
Administrator Password
This is the administrator (or root, superuser) password. You must have used it to get here.
The administrator's password can be changed here. However, the user name for this account cannot be changed: The system will accept either `root', `admin', or `administrator' as the name of this account. Add or change other user accounts here.
Admin password:
Set master password

This menu allows you to configure a number of settings, including:

**Administrator Password**
The administrator can change the default password for admin (recommended). Read and consider the comments and instructions on this menu before making any changes, as changing these features could make the unit inaccessible through Web configuration (i.e. due to firewall filtering). **NOTE** that any password changes you make will have to be entered in duplicate to prevent the chance for error.

**Idle Session Timeout**

When a login session is left unused for some time, it is prudent to disconnect the user. This applies to web login sessions (via cookies) and SSH logins. This feature may be disabled by setting the value to zero.

**Internal Firewall Setup**

As an additional layer of protection, we offer an internal firewall. When this feature is enabled, connections will only be accepted from listed hosts. For example, the administrator can key in 10.1.0.1/240 in "Accept" field, that is, the IP of the client's computer between 10.1.0.1 and 10.1.0.240 allows accessing the **CTIP-01** with the right username and password. On the other hand, the user can key in 192.168.1.0/20, for example, in "Reject" field, that is the IP of the client's computer between 192.168.1.0 and 192.168.1.20 will be rejected to access the **CTIP-01**. This makes the **CTIP-01** invisible to them. There are 3 ways to key in the IP addresses:

1. Specific IP addresses: for example, 10.1.0.1, 10.1.0.5,….
2. Net Range: for example, 10.1.0.1/240
3. Host Names: for example, yahoo.com, google.com,…

**WARNING: Be careful NOT to lock yourself out! Be certain that your IP will be accepted by your filter.**

**VNC Security Login**

When a new VNC connection is established, the remote user must be authenticated. Standard VNC protocol does not support "username"; it only supports passwords. As long as all users have unique passwords, we can infer which user is connecting based on the password provided. Alternatively, you may enable a second login screen that will require a valid username and password. This is done after the VNC connection is established using menus and prompts generated by the firmware. We call this second method "fancy login". If it is enabled, fancy login will be required from Java VNC clients as well, which is unfortunate because the one-time password scheme cannot be used, and Java VNC clients have already logged into the web server securely. Also, VNC normally encrypts passwords and uses a challenge/hashed response system that is more secure than the fancy login method. This isn't a concern if the entire connection is encrypted with SSH or SSL however.

**Access Sharing Policy**

There are 3 modes available:

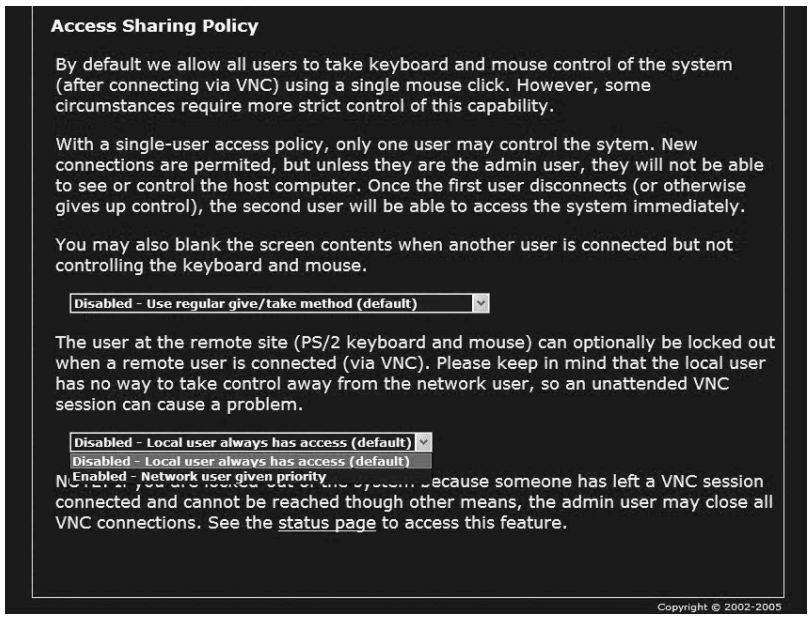
**1. Disabled– Use regular give/take method (default)**: by default we allow all users to take keyboard and mouse control of the system (after connecting via VNC) using a single mouse click.

**2. Enforce single user access policy (visible screen)**: some circumstances require more strict control of this capability, the admin user can select this mode for the highest priority access. With a single-user access policy, only one user may control the host computer. New connections are permitted, but unless they are the admin user, they will be able to view the screen ONLY, but NOT control the host computer. Once the first user disconnects (or otherwise gives up control), the second user will be able to access the system immediately.

**3. Enforce single user access policy (blank screen contents):** some circumstances require more strict control of this capability, the admin user can select this mode for the highest privacy; no one can see what the admin user is doing from the VNC screen. That is, the admin user can blank the screen contents when another user is connected but not controlling the keyboard and mouse.

With a single-user access policy, only one user may control the system. New connections are permitted, but unless they are the admin user, they will NOT be able to see or control the host computer. Once the first user disconnects (or otherwise gives up control), the second user will be able to access the system immediately.

**Local User Access Right**


Access Sharing Policy
By default we allow all users to take keyboard and mouse control of the system (after connecting via VNC) using a single mouse click. However, some circumstances require more strict control of this capability.
With a single-user access policy, only one user may control the sytem. New connections are permited, but unless they are the admin user, they will not be able to see or control the host computer. Once the first user disconnects (or otherwise gives up control), the second user will be able to access the system immediately.
You may also blank the screen contents when another user is connected but not controlling the keyboard and mouse.
Disabled - Use regular give/take method (default)
The user at the remote site (PS/2 keyboard and mouse) can optionally be locked out when a remote user is connected (via VNC). Please keep in mind that the local user has no way to take control away from the network user, so an unattended VNC session can cause a problem.
Disabled - Local user always has access (default)
Disabled - Local user always has access (default)
Enabled - Network user given priority
connected and cannot be reached though other means, the admin user may close all VNC connections. See the status page to access this feature.
Copyright © 2002-2005

There are 2 modes available:

1. **Disable – Local user always has access (default)**: under this mode, the local user has the access right to control the host computer.
2. **Enable – Network user given priority**: under this mode, the local user has NO right to control the host computer, but can view only. That is, the admin user can select this mode to lock out the local user.

## V. How to Setup your CTIP-01 with the External KVM, External Power Bar, Keyboard Mapping, and USB Keyboard/Mouse Emulation

As you get the Admin/Setup screen, please click on **Setup compatibility with host system, external KVM, external power bar**

This menu offers features that may offer enhanced functionality with certain KVM and power products. These can be left at their default values in many situations.

**External KVM Switch Brand**

Please simply select your KVM switch brand name from the list. This enables an extra shortcut key on the VNC menu to allow direct access to the KVM on-screen display (OSD) menu. Choose “Generic” if your KVM is not listed.

**Keyboard Mapping**

In many parts of the world, the keyboard has extra keys and/or different layout to better suit the local language than the default US/English layout. If your host O/S is expecting a keyboard of a special type, choose it here.

If the wrong value is used here, special language keys will not work, and some basic symbols (such as “) may not work correctly. The key layout of the “remote” keyboard must match the key layout of the “local” keyboard defined here.

**External Power Bar**

Connect a remote power control device to the serial port, and choose the model from the list. You must use the “front” serial port (DTE pin out). The rear port is reserved for setup and IPMI functions. A straight-thru cable is typically required.

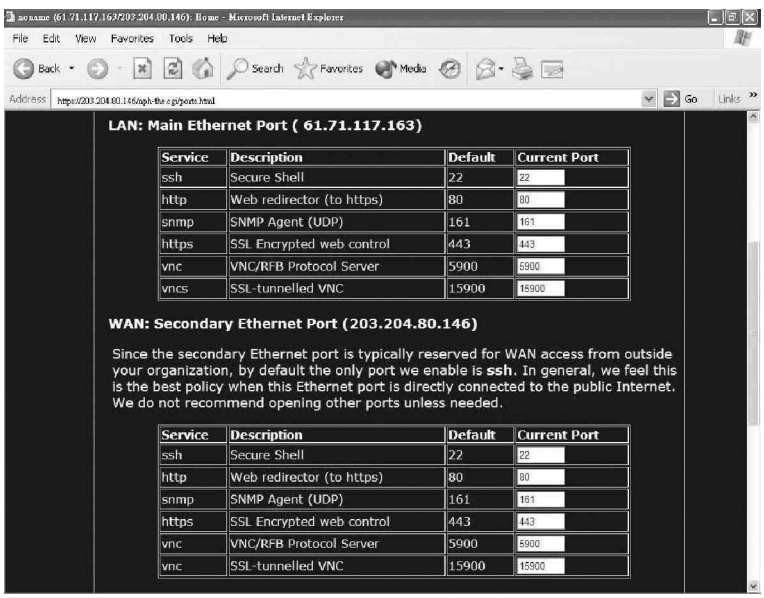
Once enabled, a status and control window will appear, individual ports can then be power controlled and monitored.

**Disable USB Keyboard/Mouse Emulation**

With this setting, you may disable the USB keyboard and mouse emulation. Under the USB emulation disabled, the USB disk emulation will still be in effect and PS/2 signals must be used for keyboard and mouse. This special mode may be required for configurations where the PS/2 keyboard and mouse are not necessarily connected to the same host as the USB cable.

## VI. How to Setup Port Numbers

As you get the Admin/Setup screen, please click on **Port numbers to be used for different services**.
This menu shows all network servers running on this machine. For the security reasons, some services may be disabled, or moved to non-standard ports.

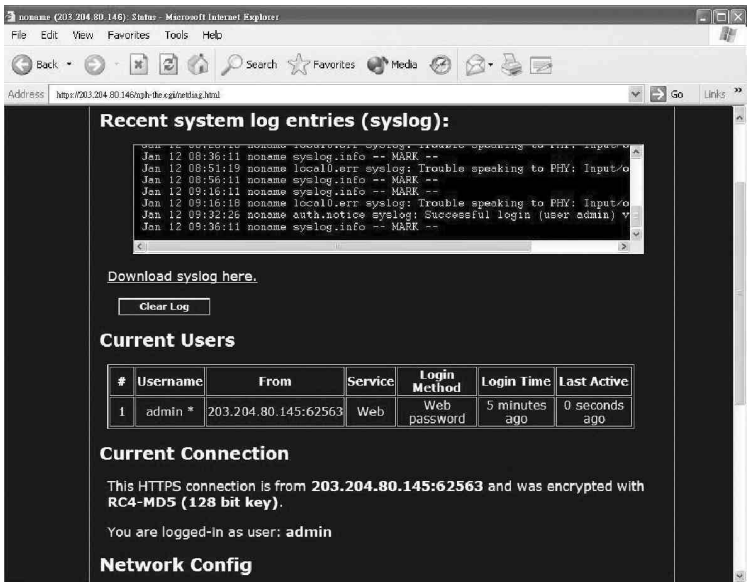

File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
LAN: Main Ethernet Port ( 61.71.117.163)
Service | Description | Default | Current Port
ssh | Secure Shell | 22 | 22
http | Web redirector (to https) | 80 | 80
snmp | SNMP Agent (UDP) | 161 | 161
https | SSL Encrypted web control | 443 | 443
vnc | VNC/RFB Protocol Server | 5900 | 5900
vncs | SSL-tunnelled VNC | 15900 | 15900
WAN: Secondary Ethernet Port (203.204.80.146)
Since the secondary Ethernet port is typically reserved for WAN access from outside your organization, by default the only port we enable is ssh. In general, we feel this is the best policy when this Ethernet port is directly connected to the public Internet. We do not recommend opening other ports unless needed.
Service | Description | Default | Current Port
ssh | Secure Shell | 22 | 22
http | Web redirector (to https) | 80 | 80
snmp | SNMP Agent (UDP) | 161 | 161
https | SSL Encrypted web control | 443 | 443
vnc | VNC/RFB Protocol Server | 5900 | 5900
vnc | SSL-tunnelled VNC | 15900 | 15900

## VII. How to Lookup your CTIP-01 System Status

As you get the Admin/Setup screen, please click on **Debug network setup values and routing**
This menu shows your **CTIP-01** system status as following:

- **Recent System Log**: it records every log entry, including what time the user logged in, what identification the user logged in, and so forth.
- **Current Users**: it shows the user's list that currently logged in.
- **Current Connection**: it shows the current IP and what encryption you are using to log in **CTIP-01**.
- **Network Config**: these tables allow you to debug network configuration problems by giving you a view into the current setup of machine.

• **Disconnect all VNC users**: in this case the users are locked-out of the system because someone has left a VNC session connected and cannot be reached through other means, the admin user can close all VNC connections.


Recent system log entries (syslog):
Jan 12 08:36:11 noname syslog.info -- MARK --
Jan 12 08:51:19 noname local0.err syslog: Trouble speaking to PHY: Input/o
Jan 12 08:56:11 noname syslog.info -- MARK --
Jan 12 09:16:11 noname syslog.info -- MARK --
Jan 12 09:16:18 noname local0.err syslog: Trouble speaking to PHY: Input/o
Jan 12 09:32:26 noname auth.notice syslog: Successful login (user admin) v
Jan 12 09:36:11 noname syslog.info -- MARK --
Download syslog here.
Clear Log
Current Users
# Username From Service Login Method Login Time Last Active
1 admin * 203.204.80.145:62563 Web Web password 5 minutes ago 0 seconds ago
Current Connection
This HTTPS connection is from 203.204.80.145:62563 and was encrypted with RC4-MD5 (128 bit key).
You are logged-in as user: admin
Network Config

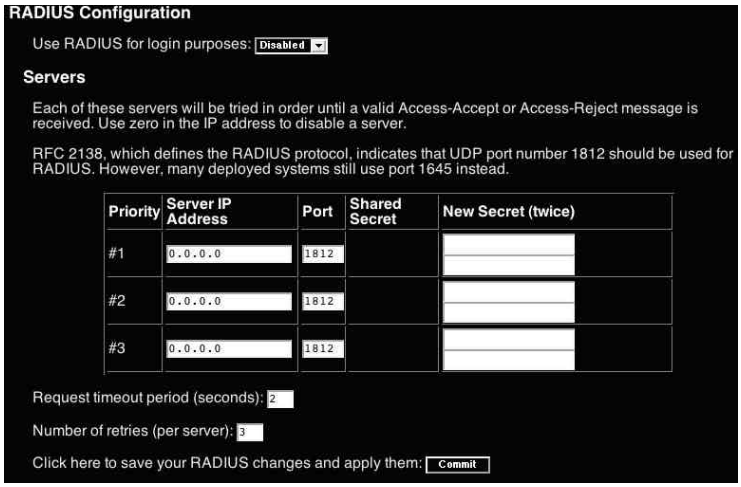
## VIII. How to Setup the SNMP Agent and Configuration

As you get the Admin/Setup screen, please click on **SNMP agent setup and configuration**

This menu allows you to configure the **CTIP-01** so it can be recognized and managed by using industry-standard Simple Network Management Protocol software.

## IX. How to Setup RADIUS authentication

As you get the Admin/Setup screen, please click on **RADIUS authentication setup**

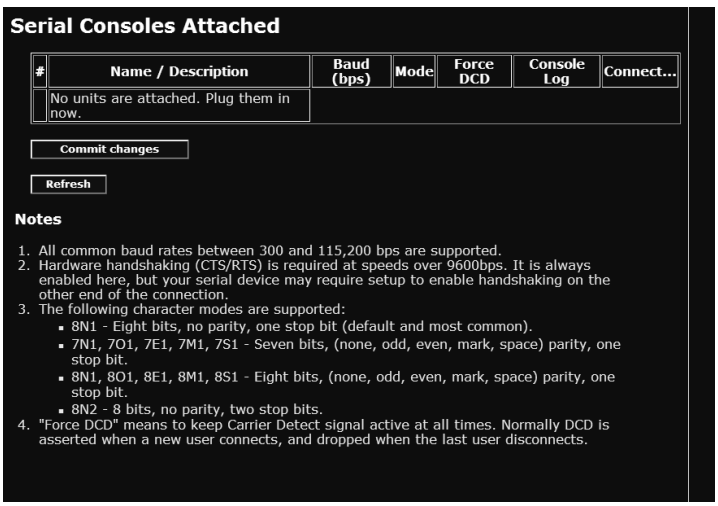

RADIUS Configuration
Use RADIUS for login purposes: Disabled
Servers
Each of these servers will be tried in order until a valid Access-Accept or Access-Reject message is received. Use zero in the IP address to disable a server.
RFC 2138, which defines the RADIUS protocol, indicates that UDP port number 1812 should be used for RADIUS. However, many deployed systems still use port 1645 instead.
Priority Server IP Address Port Shared Secret New Secret (twice)
#1 0.0.0.0 1812
#2 0.0.0.0 1812
#3 0.0.0.0 1812
Request timeout period (seconds): 2
Number of retries (per server): 3
Click here to save your RADIUS changes and apply them: Commit

The RADIUS server requires the IP address, the UDP port number (1812 - *default* or 1645) and the shared secret. The shared secret is used to encrypt communications and corresponds to a shared password for the RADIUS server and the client machine. Two additional servers may be defined for backup purposes. Each server will be tried in order, using the indicated number of retries and timeout period, which are configurable on the same page. *Remember to enable RADIUS after configuring it*. While RADIUS authentication is enabled, the locally defined accounts on the Connect-Tek over IP module will not be used, except for the SSH login. However, if a user name of the form “name.local” is given at the RADIUS prompt,

the system will use “name”; check the password locally, and skip RADIUS authentication. Delete all local accounts to avoid this behavior. When connecting via VNC, a login screen is generated that asks for a RADIUS username and password.

## X. How to Setup and Control the External Serial Consoles

As you get the Admin/Setup screen, please click on **External Serial consoles setup and control**


Serial Consoles Attached
#
Name / Description
Baud (bps)
Mode
Force DCD
Console Log
Connect...
No units are attached. Plug them in now.
Commit changes
Refresh
Notes
1. All common baud rates between 300 and 115,200 bps are supported.
2. Hardware handshaking (CTS/RTS) is required at speeds over 9600bps. It is always enabled here, but your serial device may require setup to enable handshaking on the other end of the connection.
3. The following character modes are supported:
8N1 - Eight bits, no parity, one stop bit (default and most common).
7N1, 7O1, 7E1, 7M1, 7S1 - Seven bits, (none, odd, even, mark, space) parity, one stop bit.
8N1, 8O1, 8E1, 8M1, 8S1 - Eight bits, (none, odd, even, mark, space) parity, one stop bit.
8N2 - 8 bits, no parity, two stop bits.
4. "Force DCD" means to keep Carrier Detect signal active at all times. Normally DCD is asserted when a new user connects, and dropped when the last user disconnects.

There are two ways that **CTIP-01** can control the serial devices such as power bar, router, printer, and so on. The first way is connect the serial devices with the **DTE** serial port or **DCE** serial port of **CTIP-01**, and the second way is connect the serial devices with the serial port of **Serial Supervisor**. For more information, refer to **Appendix D**.

## XI. How to Set Date and Time

As you get the Admin/Setup screen, please click on **Set date and time**

Allows you to set your **CTIP-01** to **Local Time** or **Universal Coordinated Time** (GMT). Date and time is stored without consideration for time zone. If you are controlling multiple sites in different time zones, we recommend you use GMT for all machines.

## XII. How to Update your Firmware

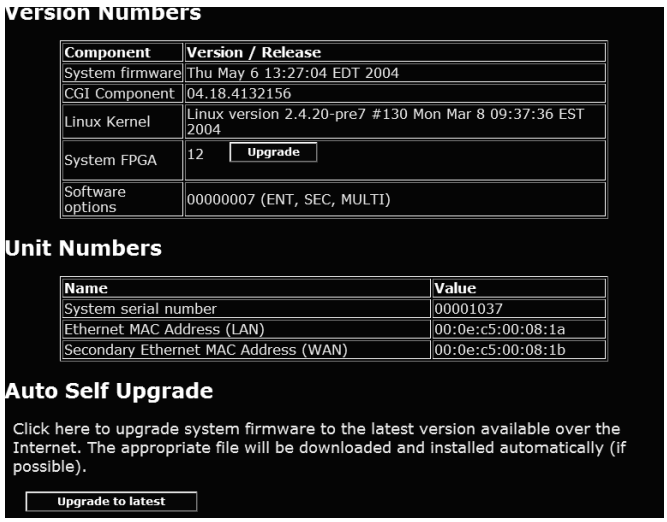
As you get the Admin/Setup screen, please click on **Firmware and flash memory management**

The firmware of **CTIP-01** is online upgradable. When upgrading to the latest version, please login as admin--only the administrator has rights to do so.

**Auto Self Upgrade**

The **CTIP-01** includes an innovative feature allowing the unit to upgrade itself over the Internet. Simply click on the button labeled “Upgrade to Latest” and the unit will go out to the Internet and download the latest version of the system firmware and then install it. If the unit cannot access the Internet directly (perhaps due to a web proxy or other firewalls), then a page will be shown that allows your browser to download the required file. Save this file to disk and then upload it as described in the next section, Manual Upload. The main FPGA is upgraded separately, and has its own Get latest button. This file is unique for each unit, so it must be done in this manner.

If you have multiple units to upgrade, you may choose the “Get latest version” button that will not attempt to upgrade the unit directly, but will instead locate the required file. This file can be uploaded to multiple units manually.




**Manual Upload**
Enter the name of the firmware file that you received from **Connect-Tek** into the field provided (or use the Browse... button). Press Start Upload and wait until a successful upload message is shown.

**NOTE**: Remember the following during the firmware upgrade…

- Do NOT turn off power to unit before this operation completes successfully. It may take several minutes to write to flash memory.
- The unit will sometimes reboot as part of the upgrade procedure, depending on which system component is upgraded. You will have to reconnect and re-login in those cases.
- Wait at least two minutes after pressing Start. Do not assume the upload did not work. There is no status indicator bar to show the progress of the upload. The upload could simply be slow.
- Each file that is distributed upgrades a different component of the system. Therefore, be sure to apply all files you are given as part of an upgrade. The system knows what to do with each file you give it, and they are checked for validity before being applied.

## XIII. How to Upload Custom Certificate

As you get the Admin/Setup screen, please click on **Firmware and flash memory management**, and then scroll down the bottom of the screen.

Upload your own certificate to replace the factory-supplied SSL certificate here.
We require an RSA private key and corresponding public certificate to be combined together into one PEM file. There should be no encryption on the private key and it must be first in the file. Therefore, we expect a text file in this format:

```
-----BEGIN RSA PRIVATE KEY-----
[based64 encoded key]
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
[based64 encoded certificate]
-----END CERTIFICATE-----
[end of file]
```

Uploading the root CA public certificate is optional and only affects the link on the login page. It does not affect operation otherwise. It is just a X.509 PEM file holding a public certificate.

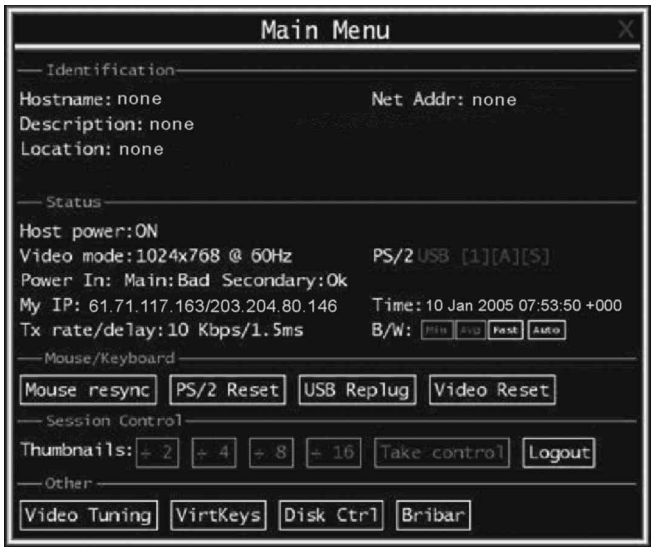
## XIV. How to Speed Up your CTIP-01

As you login the **CTIP-01** with the right username and password, you will get the following screen:

Please simply double click on the small square window in the middle of the screen. You'll get the VNC screen. That is, you will see the screen of the host computer, please scroll the screen to the bottom. It is the Bribar (refer to Chapter 5, Section C) in that lower area. Please click on Menu (refer to Chapter 5, Section D) of the Bribar.

**NOTE**: You may need to upgrade or download your Java support in your browser before using the VNC screen to remote control the host computer; however, most modern browsers come with a version of Java that is compatible with this application.

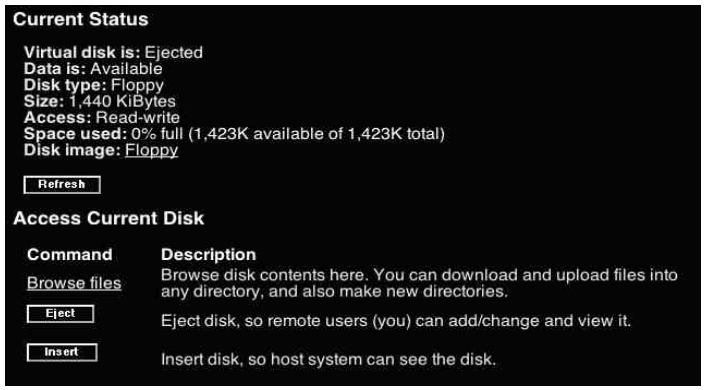
From this screen, you can do the bandwidth control. There are 4 modes available: Min, Avg, Max, and Auto. The white button is the mode that the system is currently operating. If you choose Min/Avg/Max then you will override the default, Auto. As the automatic mode measures actual network performance, you may see the current mode switch from Min up to Avg or Max. The different modes indicate more time spent on compression versus more bandwidth. There is no visual difference between the modes, but there can be a noticeable difference in speed and smoothness.



# Chapter 4 File Transfer

## A. The File Transfer Screen

The **CTIP-01** is able to emulate a virtual disk drive attached to the host via USB, and must have the ***optional USB cable*** connected to the **CTIP-01** and the host computer to function. Depending on configuration, it will appear to the host as a floppy drive (1.44MB), an 8MB RAM disk or a CD-ROM. The host computer does not require any special drivers or other configuration. It just looks like a new USB drive. You can transfer files onto the virtual disk while it is "ejected" and then "insert" the disk so the host can see the files. Any files the host writes to the disk can be retrieved once the disk is "ejected".


Current Status
Virtual disk is: Ejected
Data is: Available
Disk type: Floppy
Size: 1,440 KiBytes
Access: Read-write
Space used: 0% full (1,423K available of 1,423K total)
Disk image: Floppy
Refresh
Access Current Disk
Command
Description
Browse files
Browse disk contents here. You can download and upload files into any directory, and also make new directories.
Eject
Eject disk, so remote users (you) can add/change and view it.
Insert
Insert disk, so host system can see the disk.

Access to the files is performed through the web interface. The disk may be inserted from either the web interface, or the Disk Control menu available via VNC. Most operating systems can "Eject" the disk once it is inserted, but it can also be ejected from the Web or VNC.

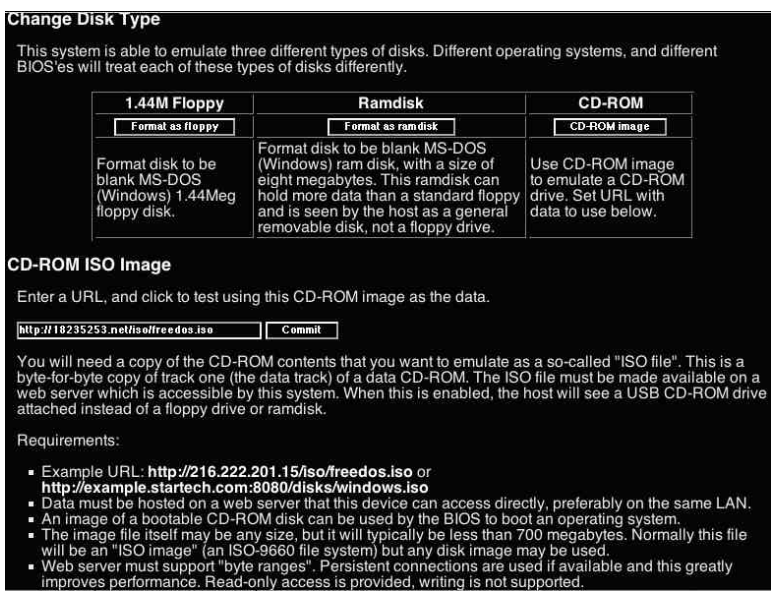
When emulating a floppy disk or RAM disk, the data is stored in RAM on the **CTIP-01** itself. In order to emulate a CD-ROM disk drive, a web server is required to provide the CD-ROM image data. The web server must be accessible to the module, which communicates with it constantly as data is needed.

## B. Floppy Mode

**Step 1**. Choose the Format as Floppy button to switch to floppy mode.

**Step 2**. Under Windows, the drive will be identified as a "high density floppy" and will typically be assigned a drive letter of "B:". The capacity is limited to 1.44 megabytes in this mode.

The purpose of supporting floppy mode is to permit the use of floppy-disk images generated by other systems. For example, the flash BIOS upgrade process is performed with a special floppy and is bootable. You can transfer bits from that floppy to the **CTIP-01** (use the upload disk image form). Now, you can boot from the special floppy. In addition, emergency repair disks are often restricted to floppies.


Change Disk Type
This system is able to emulate three different types of disks. Different operating systems, and different BIOS'es will treat each of these types of disks differently.
1.44M Floppy
Ramdisk
CD-ROM
Format as floppy
Format as ramdisk
CD-ROM image
Format disk to be blank MS-DOS (Windows) 1.44Meg floppy disk.
Format disk to be blank MS-DOS (Windows) ram disk, with a size of eight megabytes. This ramdisk can hold more data than a standard floppy and is seen by the host as a general removable disk, not a floppy drive.
Use CD-ROM image to emulate a CD-ROM drive. Set URL with data to use below.
CD-ROM ISO Image
Enter a URL, and click to test using this CD-ROM image as the data.
http://18235253.net/iso/freedos.iso
Commit
You will need a copy of the CD-ROM contents that you want to emulate as a so-called "ISO file". This is a byte-for-byte copy of track one (the data track) of a data CD-ROM. The ISO file must be made available on a web server which is accessible by this system. When this is enabled, the host will see a USB CD-ROM drive attached instead of a floppy drive or ramdisk.
Requirements:
Example URL: http://216.222.201.15/iso/freedos.iso or http://example.startech.com:8080/disks/windows.iso
Data must be hosted on a web server that this device can access directly, preferably on the same LAN.
An image of a bootable CD-ROM disk can be used by the BIOS to boot an operating system.
The image file itself may be any size, but it will typically be less than 700 megabytes. Normally this file will be an "ISO image" (an ISO-9660 file system) but any disk image may be used.
Web server must support "byte ranges". Persistent connections are used if available and this greatly improves performance. Read-only access is provided, writing is not supported.

## C. RAM Disk Mode

**Step 1**. Choose the Format as Ramdisk button to switch to RAM disk mode.
**Step 2**. This mode is intended to facilitate simple data transfer between the remote user and the host computer.
**Step 3**. It will be recognized by Windows as an eight megabyte removable disk and assigned a drive letter.
**Step 4**. You can easily drag and drop files up to 8MB in size to this device.
**Step 5**. In Windows explorer, you can choose the "Eject" option to make the data available to the remote users.

***Reading files from disk***
On the File Transfer menu, make sure the disk is "ejected," then choose the Browse files link. A web page will be generated that shows the root directory on the disk. You can download files to your browser by clicking on the file name. It is also possible to delete files and create directories using the buttons provided on that page.

***Disk Formats***
When you choose the Format as... button, the disk image stored in RAM is formatted to be an empty MS-DOS disk, with a single file called Put files here...TXT. The **CTIP-01** is able to read most MS-DOS/Windows formatted disks and presents the files via the web interface. However, disk emulation occurs at the lowest level so that other disk formats can be used, if you have the tools needed to create and read the disk images. At the bottom of the page are the upload and download options for the entire disk image. Any image that is exactly 1,474,560 bytes long will be treated as a floppy. Images of other sizes are supported up to 8MB.

## D. CD-ROM Mode

The **CTIP-01** does not store any data in this mode. Instead, it emulates a USB CD-ROM drive with a disk inserted. The data from that disk must be provided by an external web server.
**Step 1**. You will need a copy of the CD-ROM contents that you want to emulate as an ISO file. This is a byte-for-byte copy of track one (the data track) of a data CD-ROM. The ISO file must be made available on a web server which is accessible by the **CTIP-01**.
**Step 2**. Switch to CD-ROM mode, type in a URL pointing to the ISO image, and click on "Commit".
**Step 3**. The system will connect to the web server and test the file for access. If successful, you will be shown a short report on the file contents, and the disk will be ready to use. Currently there is no other way to preview or browse the contents of the CD-ROM image, except from the host.

***CD-ROM Web Server Requirements:***
- **1**. Data must be hosted on a web server that the **CTIP-01** can access directly, preferably on the same **LAN**.
- **2**. An image of a bootable CD-ROM disk can be used by the BIOS to boot an operating system.
- **3**. The image file itself may be any size, but it will typically be less than 700 megabytes. Normally this file will be an ISO image (an ISO-9660 file system) but any disk image may be used.
- **4**. Web server must support "byte ranges". Persistent connections are used, if available, as this greatly improves performance. "Read-only" access is provided; writing is not supported.

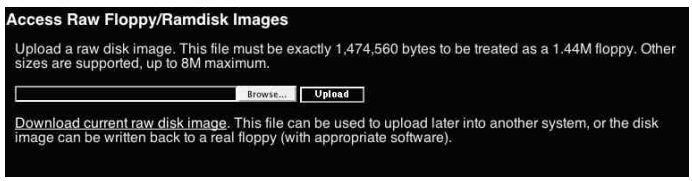
## E. How to Remotely Boot your Computer

If the host machine's BIOS support USB boot devices, it is possible to boot from the emulated CD-ROM or floppy. This allows complete operating system replacement without any on-site intervention.

**Step 1**. Get a bootable disk image onto the emulated floppy or CD-ROM. If you would like to use it as the CD-ROM mode, follow Step 2a. Alternatively, you can also use it as the floppy mode, by referring to Step 2b.

**Step 2** **a**. For CD-ROM images, you will need an ISO image from a disk that contains special bits to enable boot ("El Torito" standard). Nothing special is needed when reading the ISO from a working, bootable CD-ROM.

**b**. To create a bootable floppy, you can format the emulated floppy from the target system, or read the data from a working boot floppy. This can be done from Windows using "Disk Copy" (right click on the drive letter in the Windows Explorer) or by using a program like "RAWRITE".


Access Raw Floppy/Ramdisk Images
Upload a raw disk image. This file must be exactly 1,474,560 bytes to be treated as a 1.44M floppy. Other sizes are supported, up to 8M maximum.
Browse...
Upload
Download current raw disk image. This file can be used to upload later into another system, or the disk image can be written back to a real floppy (with appropriate software).

**Step 3**. Once you have a bootable image (CD-ROM or floppy) working on the Connect-Tek over IP module, you must adjust your BIOS settings to tell it to boot from a USB device.

**NOTE**: You must select "USB CD-ROM" as the boot device for the BIOS, if using a CD-ROM image and "USB Floppy" if using a floppy image.

***BIOS and OS Vendor Support***

**NOTE**: Up-to-date information about OS and BIOS support is listed in the on-line help page of the internal web server.

**Windows 95 or earlier**: No USB support.

**Windows 98:** Keyboard and mouse are supported. Floppy/CD-ROM disk emulation is not supported.

**Windows 2000 SP3+:** Keyboard and mouse are supported. A bug in versions before Service Pack 2 prevents floppy/CD-ROM support from working correctly. (In particular, it appears to work, until you attempt to transfer files bigger than 4096 bytes). Upgrade to SP3 or later for full disk emulation support.

**Windows XP, Windows Server 2003:** Keyboard, mouse and disk emulation are supported.

**FreeBSD 4.5:** Keyboard, CD-ROM tested and working; other features untested.

**AMIBIOS (from American Megatends Inc):** Keyboard, floppy and CD-ROM emulation work well. It is possible to boot from virtual CD-ROM or Floppy. You must enable either the USB floppy or CD-ROM as a boot device (under Advanced Setup) and enable "USB Function for DOS" (under Features Setup).

**Award BIOS (from Phoenix Technologies):** USB Keyboard works. USB booting is not implemented by this BIOS, although it is listed in the menus.

**NOTE:** BIOS firmware is constantly evolving. Contact your computer or BIOS manufacturer for the latest release of your computer's BIOS for maximum functionality.

# Chapter 5 How to Remotely Control the Host Computer

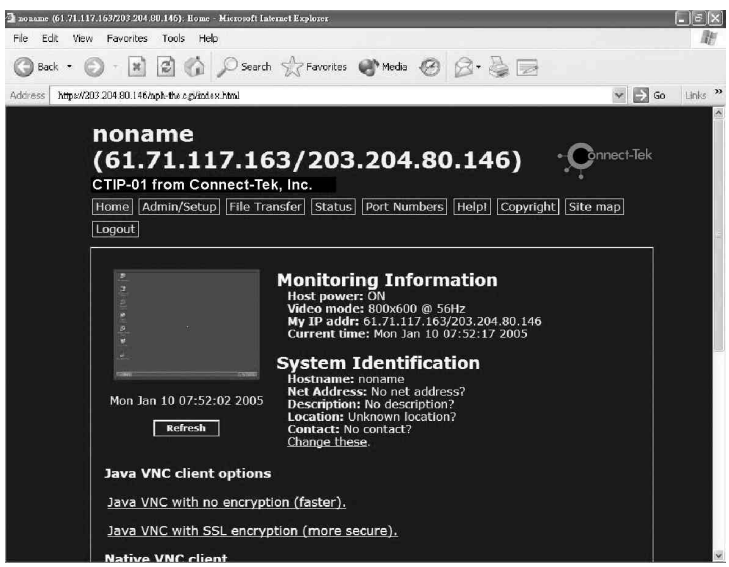
## A. Accessing the VNC Interface

There are three ways to communicate with the **CTIP-01** in order to control the host computer.

- **Web interface**: The integrated Web server includes a Java-based VNC client. This allows easy browser-based remote control.
- **Native VNC client**: There are several third-party software programs that use the standard VNC protocol, available in open source and commercial VNC clients.
- **SSH access**: By default, there is a standard SSH server running on port 22 (the standard SSH port). Once connected via SSH, the VNC traffic is tunneled through the SSH connection and encrypts the VNC session. Each method will be discussed briefly in the following section. The type of encryption method or client used is not critical.

### I. Web Interface

The Java-based VNC client that is integrated into the **CTIP-01**'s interface requires a browser with cookies and JavaScript enabled. To start the Java VNC client, login to the Web configuration interface and click on the thumbnail of the desktop on the **Home** menu, or follow one of the two links on that page:
Java VNC with no encryption (faster).
Java VNC with SSL encryption (more secure).




**You may need to upgrade or download your Java support in your browser before using the VNC screen to remote control the host computer**; however, most modern browsers come with a version of Java that is compatible with this application.
The Java VNC client makes a connection back to the Connect-Tek over IP module over port 5900 (by default) or 15900, if encrypted. The encrypted connection is a standard SSL (Secure Socket Layer) encrypted link that encrypts all data from the session, including the actual video pictures.

Because Java is considered a "safe" programming language, the Java VNC client has some limitations. Certain special keystrokes cannot be sent, such as "**Scroll Lock**" on the keyboard.

This client software requires the use of Java 2 (JRE 1.4) to enable features like wheel mouse support. Sun Microsystems's Java site, www.java.com, is an excellent resource to ensure your browser and operating system is up-to-date.

### II. Native VNC Client

This system implements the VNC protocol, so any off the shelf VNC client can be used. There are over 17 different VNC clients available and they should all work with this system. This system automatically detects

and makes use of certain extensions to the basic RFB protocol that is provided by the better VNC clients.

The best client currently is TightVNC (www.tightvnc.com). Binaries are available for Windows, Linux, MacOS and many versions of Unix. Source code for all clients is available there too. This version of VNC is being actively developed.

The authoritative version of VNC is available from RealVNC (www.realvnc.com). This source base is the original version of VNC, maintained by the original developers of the standard.

For a commercial, supported version of VNC, you should consider TridiaVNC (www.tridiavnc.com). Their version of VNC is a superset of TightVNC and contains a number of enhancements for use in a larger corporate environment.

**NOTE**: Some native VNC clients may require a flag or setting indicating they should use BGR233 encoding by default. If this flag is not set, you may see a garbled picture and the client will fail. The Unix versions of VNC require the flag -bgr233. For examples on using this flag, review the commands in the following section.

**III. SSH Tunnel (with Native VNC client)**

If you are using openssh, here is the appropriate Unix command to use, based on the default settings on a machine at 61.71.117.163:

```
ssh -f -l admin -L 15900:127.0.0.1:5900 61.71.117.163 sleep 60
vncviewer -bgr233 127.0.0.1::15900
```

Same command, but using the **WAN** port:

```
ssh -f -l admin -L 15900:127.0.0.1:5900 203.204.80.148 sleep 60
vncviewer -bgr233 127.0.0.1::15900
```

**NOTE:** A copy of these commands, with appropriate values filled in for your current system setting, is provided in the *on-line help* page. This allows you to “cut-and-paste” the required commands accordingly.

You have 60 seconds to type the second command before the SSH connection will be terminated.

The port number “15900” is arbitrary in the above example and can be any number (1025...65535). It is the port number used on your client machine to connect your local SSH instance with the VNC client. If you want to tunnel two or more systems, you will need to use a unique number for each instance on the same SSH client machine.

Some Unix versions of the VNC client have integrated SSH tunneling support. Some clients require your local user id to be the same as the user id on the system.

Use a command like this: vncviewer -bgr233 -tunnel 61.71.117.163:22

## B. Using the VNC Menu

One of the unique features of this product is the VNC menu system. Whenever you see a window with a dark blue background and gray edges, this window has been inserted into the VNC data stream so that it is effectively laid over the existing video. These menus allow you to control the many features of the **CTIP-01** without using the web interface or a custom client.

**Welcome Window**

When you initially connect to the system, a window similar to the above one will be shown.

This tells you which system you are controlling, what encryption algorithm was used and what key strength is currently in effect. Click anywhere inside the window to clear it, or wait ten seconds.

## C. How to Use the Bribar

Along the bottom of the VNC screen is a dark blue bar with various buttons. We call this feature “the bribar”. Its purpose is to show a number of critical status values and to provide shortcuts to commonly used features. Here is a snapshot of what it may look like. There will be slight differences based on optional features and system configuration. Starting from the left side of the Bribar, each feature and its function is outlined below.

**Bandwidth:** Indicates current average bandwidth coming out of the Connect-Tek over IP module. The second number measures round trip time (RTT) of the connection when it was first established.

**Resync:** Re-aligns the remote and local mouse points so they are on top of each other.

**Redraw:** Redraws the entire screen contents; occurs immediately.

**Video Adjust:** Adjusts the video phase automatically.

**PS/2:** Resets the PS/2 keyboard and mouse emulation. Useful to recover failed mouse and/or keyboard connections in PS/2 mode.

**USB:** Resets the USB connection by simulating an unplug and replug. Forces operating system to recognize the USB keyboard, mouse and emulated disk drive.

**÷4, ÷8:** Switches to thumbnail mode, at indicated size.

**Ctrl-Alt-Del:** Sends this key sequence to the host. Works immediately.

**Alt-F4:** Sends the key sequence to host (closes windows).

**Menu:** Shows the Main Menu, refers to Chapter 5, Section D for more information.

**Video:** Shows the video-tuning menu where the picture quality can be adjusted, refer to Chapter 5, Section F for more information.

**Keys:** Shows the VirtKeys menu, which allows you to simulate pressing special keys such as the Windows key or complex multi-key sequences, refer to Chapter 5, Section F for more information.

**Disk:** Shows the USB emulated disk menu.

**In/Ej:** Insert or eject the emulated USB disk. Enabled only if the host is recognizing the USB disk.

**R/W:** Shows if the disk image is readable and/or writeable. If the disk is readable, the letter **R** will be white. Whenever the host reads from the disk, the letter **R** will glow green for a few seconds. Whenever the host is writing to the disk, the letter **W** will glow for a few seconds.

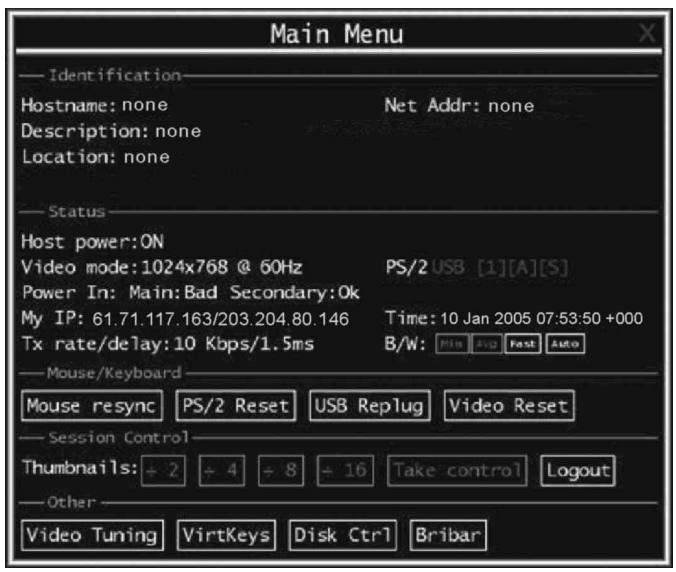
**8M:** The type of USB disk selected is indicated here. In the example, it is an eight-megabyte Ramdisk. The letters **Flpy** indicate floppy disk and **CD** indicates emulated CD-ROM.

**PS/2:** This area will show either PS/2 (as in this example) or USB to indicate if keyboard and mouse

are being emulated via USB connection or PS/2 signals. If Autosync appears beneath this indicator, the mouse pointers on the local mouse and the VNC session will be synchronized automatically.
**[1][A][S]:** These flags show the state of the keyboard lights, NumLock, ShiftLock and ScrollLock respectively.
**X:** Click this button to close the Bribar and hide it. This can be very useful on a client machine whose screen-size is the same as the remote machine. No vertical screen space is wasted with the Bribar. Use double-F7 to start the main menu, and then click on Bribar to restore the feature.
**Other items:** If the server's screen is larger than 1024x768, additional buttons will be shown to the right of the above listed items. These are all keyboard shortcuts and are duplicated in the Keys menu.

## D. How to Use the Main Menu

To access the main menu, press F7 twice quickly. You must press the key twice within one second. If you press it once or too slowly, then the F7 key(s) are sent to the host, just like any other key. This is the only way to get into the menu system, if the Bribar is disabled. Here is the main menu for a typical system:



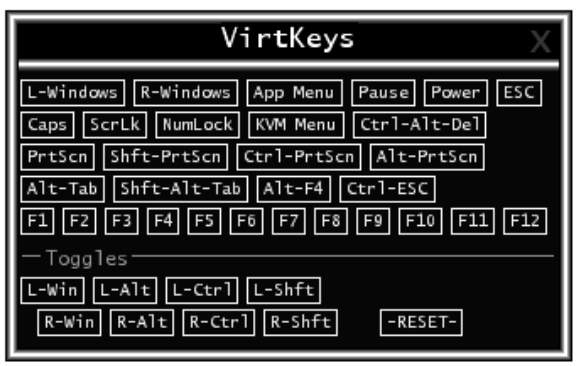

The main menu window may be moved by clicking and dragging on the title bar. It can be closed by pressing Escape, or by clicking on the red X in the top right corner.
Here is a guide outlining various fields from the Main Menu. Most of the functions operate immediately. Other functions require a response to a confirmation prompt first before performing the requested function.

- **Identification:** Fixed text label that is defined by the user in the Web interface. This does not affect the operation of the system and is intended to assist with administration.
- **Status:** Current status of the attached system and the status of the module.
- **B/W Min/Avg/Max/Auto:** Bandwidth control. The white button is the mode the system is currently operating. If you choose Min/Avg/Max then you will override the default, Auto. As the automatic mode measures actual network performance, you may see the current mode switch from Min up to Avg or Max. The different modes indicate more time spent on compression versus more bandwidth. There is no visual difference between the modes, but there can be a noticeable difference in speed and smoothness.
- **Mouse Resync:** Resynchronizes the mouse pointer so that the local and remote mouse pointers are on top of each other.
- **PS/2 Reset:** Resets the PS/2 emulation going to the host and to the attached PS/2 devices. This can be used if the mouse stops responding or the PS/2 keyboard isn't working.
- **USB Replug:** Simulates unplugging the USB connector and then plugging it back in. If the host is not recognizing USB input devices, this button may be used to restore functionality.
- **Take Control:** When multiple users are connected to the same system, use this button to take control away from another user. Only one user may control the keyboard and mouse at any time. All users see the same picture.

- Thumbnails: Switch to smaller thumbnail size screen images (click anywhere on thumbnail to restore it). Each button corresponds to a different sized image, from half size to one-sixteenth.
- **Logout:** End the VNC login session and disconnect.
- **Video Tuning:** Sub-menu with video adjustments, to be used when automatic picture adjustment does not provide a good quality picture (see section below).
- **VirtKeys:** Virtual keyboard provides a menu with special keys that are often hard to generate but needed by the remote system. The most common key sequence is the [Ctrl] – [Alt] – [Del] (see section below).
- **Disk Ctrl:** Emulated USB disk control submenu. Shows status of floppy/Ramdisk or CD-ROM and permits easy "insertion" or "eject". (See section below.)
- **KVM Menu:** Generates the key sequence used to access the on-screen menu for an enterprise-class KVM switch. When these conventional KVM switches are combined with the **CTIP-01**, this key makes accessing their built-in menu easier, especially from the Java client. This button will only be shown when an external KVM has been enabled via the web interface.
- **Bribar:** Closes or reopens the Bribar window along the bottom of the screen.

## E. How to Use the VirtKeys Menu

This is a snapshot of the Virtual Keys window:



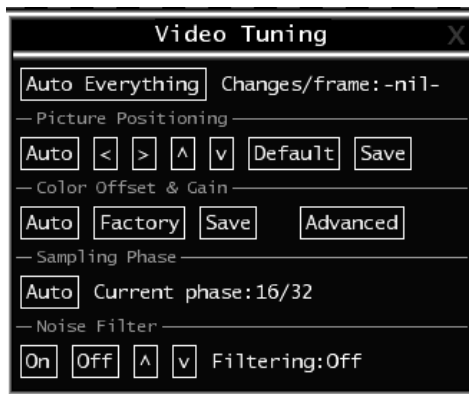

Clicking any button in the top half of the window simulates pressing and releasing the indicated key. In the bottom area of the screen, clicking will simulate the indicated Meta key being pressed. You may then click in the top part to send another key and release the Meta key at the same time. Alternatively, you may move the mouse outside this window, press the regular key, and then choose -RESET- to release all depressed keys.
The VirtKeys menu can be left open while using the host system. You can then click the required button at the suitable time, and still interact with the host in a normal fashion.

Examples:

- **[Ctrl]-[Alt]-[F4]:** Use L-Ctrl then L-Alt in the Toggles area. Then click F4.
- **To bring up the Start menu under Windows:** Click the L-Windows button at the top left of the above window.

## F. How to Use the Video Tuning Menu

This menu is used to fine-tune the video picture.




**Auto Everything:** use this button to automatically fine-tune all three adjustments. If the test pattern for Color Offset calibration is not present on the screen, then the Color Offset adjustment is skipped.

**Changes/frame:** it indicates the number of 16x16 blocks of video that are being sent, on average, for every frame of video. With a static image being displayed by the server, this number will be zero (shown as -nil-). Moving the mouse, for example, will cause the number to jump to about 2 or 3. You may use this number to judge the picture quality as you adjust the controls on this menu.

**Picture Positioning:** it effects the image position on your screen. If you see a black line on either side of your screen, or at the top or bottom, you can use the arrow buttons to shift the image in that direction. Pressing Auto does the same thing for you automatically. Use Save to save the changes you have made manually. Since this adjustment depends on the video mode, separate values are stored for each video mode.

**Color Offset:** it is a fine tuning adjustment that requires the use of a test pattern. There is a copy of the test pattern available on the Help! menu of the integrated web server. You must arrange for that image to be shown on the host computer. Do not allow scaling, cropping or any other changes to that image. Press the Auto button and the system will calibrate color for the best possible picture in approximately one minute. If the system cannot find the test pattern on the screen, it will say so. Check that the pattern isn't scaled or covered up. It's important to do this operation in 24-bit or 32-bit color video mode (i.e. true color). Although the algorithm may work in 16-bit or 8-bit color video modes, the results will not be optimum and usually it won't be able to recognize the test pattern.

**Advanced:** pressing this button will open the Advanced Video Tuning menu. While the vast majority of users will not need to adjust these settings, it offers a high-degree of control of the video settings of your VNC sessions.

**Sampling Phase:** this does not normally need to be used since our system tunes the sampling phase whenever the video mode changes. This button does not require a test pattern, but will perform optimally when used with our standard test pattern. For your reference, the sampling phase number is shown to the right of the Filtering button.

**Noise Filter:** it controls the advanced video filtering of our system. Unlike other filtering algorithms, our noise filter will only remove noise. It does not degrade the signal quality or readability of small text. You may turn it

on and off using the indicated button, or set it to other values using the arrows. Higher numbers cause more filtering and may cause artifacts when moving windows. *The most common visual artifact is a vertical line dropping when moving windows horizontally.* You may use the Redraw button to correct these, or use a lower filter number. At minimum, these values must be greater than two.

## G. Disk Control Menu

Here is a picture of the Disk Control Menu, while using a CD-ROM image:

Aside from status information, there are only three buttons in this window. Insert and Eject will simulate that action, and only one option is enabled at any time, based on the current state of the emulated disk. USB Replug can be used to force the host to recognize the disk. It is not needed unless the host OS or hardware does not recognize it automatically.

## Appendix A Troubleshooting

If you are experiencing trouble with your devices, first make sure that all cables are connected to their proper ports and are firmly seated.

**I can't connect to the CTIP-01.**
**Step 1**. Check if the network connection is working (ping the IP address of **CTIP-01**). If not, check network hardware. Is **CTIP-01** powered on? Check if the IP address of **CTIP-01** and all other IP related settings are correct. Also verify that all the IP infrastructure of your **LAN**, like routers are correctly configured. Without a ping functioning, **CTIP-01** can't work. If it still can't connect to the **CTIP-01**, please go on to the next step.
**Step 2**. Refer to the **Quick Start Guide**, choosing the third way: **Using the HyperTerminal via Serial Port,** and type "**F**" to reset everything back to the factory defaults. Then, setup the IP address, netmask, and default gateway. And then, type "**W**" to record the changes to the memory.

**I can't login via SSH.**
Was the correct user and password given? The default username and password as shipped from the factory is username admin with a password of admin. Configure your browser to accept cookies. The user name and password are case sensitive, check the status of the Caps Lock on your keyboard. If you see a warning about "identity of host cannot be verified", and a question about saving the host's fingerprint, this is normal for the first time you connect to any machine running SSH. You should answer "yes" so that your SSH client saves the public key of this host and doesn't re-issue this warning.

**I can't remember the Master Password.**
Reset the master password. Please refer to **Quick Start Guide,** choosing the third way**: Using the HyperTerminal via Serial Port** . Use the **S** command, and type a new password. The old password is not required for this procedure. And, **please remember to type "W" after you made any change.**

**The mouse on the remote site does not work or is not synchronized.**
a. Make sure there is only one mouse driver installed in each computer.
b. Set the mouse acceleration to 'None' in the host mouse driver properties.
c. Windows XP has a setting called 'Enhance pointer precision'. This should be disabled for correct mouse synchronization.

**Remote mouse and local mouse don't line up.**
Use the "mouse resync" command in the main menu or press the "Resync" button on the Bribar. If the mouse pointers still don't line up, verify that mouse acceleration has been disabled.

**NOTE**: **The Windows login screen does not accept the "mouse acceleration" option, and always has the mouse accelerated regardless of your configuration. Therefore, on this screen it is best to avoid using the mouse.**

**After "Resync", the mouse on the remote site is synchronized, but there is small constant offset between remote and local mouse cursors.**
This is a video position error. Normally a slight video positioning error is perceived as a mouse sync issue. A video positioning error is visible as a black line along the top or bottom (and right or left) edges of the remote screen. On the "Video Tuning" menu (please see the diagram on page Chapter 5, Section F.), use the arrows under "Picture Positioning" to move the screen until the two pointers exactly line up. ***Remember to save your position changes!***

**Monitor works, but keyboard and mouse do not.**
Make sure you haven't swapped the keyboard and mouse cables

**VGA image is not clear.**
You may be using poor quality VGA cables. Make sure you are using UL-2919 rated, double-shielded VGA cables.

**The quality of video is bad or the picture is grainy.**
a. Use the brightness and contrast settings.
b. Use the auto adjustment feature to correct a flickering video.
c. Also, try the "Auto everything" button on the "Video Tuning" menu refers to the diagram on page Chapter 5, Section F.
d. Display the test pattern on the host and use "Auto Everything".
e. Try a lower refresh rate (60Hz is best)
f. Enable the noise filter and set to higher value.
g. Use lower resolution if possible (1024x768)
h. Reduce number of colors (8-bit or 16-bit color instead of 24/32).
i. Use a better quality video card.

**There is a keyboard error on boot.**
You may have a loose keyboard connection. Make sure your keyboard cables are well-seated.

**The letters on the TFT LCD display are blurry or have shadows.**
You may have improper resolution settings. Under the Control Panel, set the VGA output of your computers to match the highest resolution of the LCD monitor with Large Font selected.

**Certificate warning shown while connecting via HTTPS.**
It is normal for a warning dialog to be shown when connecting via HTTPS. The SSL certificate we use is created when the unit is first produced. It does not contain the correct hostname (subject name) because you can change the hostname as required. Also, it is not signed by a recognized certificate authority (CA) but is signed by our own signing authority.

**Windows XP doesn't awake from standby mode.**
This is possibly a Windows XP problem. Try not to move the mouse while XP goes into standby mode.

**The terminal connection to CTIP-01 for initial configuration cannot be established.**
Check that the straight-through, 9-pin RS-232 cable connected to DCE Serial Port of the **CTIP-01** and HyperTerminal software is set to the following line parameters:
Connection speed: 115200 bps
No. of bits: 8
Parity: None
Stop bits: 1
Flow Control: None
Connect the computer to the **CTIP-01** and power this computer on. Then, power on the **CTIP-01**. Also, Windows HyperTerminal has a bug: if you change baud rates while connected, the screen is updated but the hardware is still at old baud rate; hang up and reconnect (using icons at top of screen) to make new settings take effect.

**If my network has a firewall, what setting do I use on the IP Extender to open a port into the network?**
You shouldn't change any settings in the **CTIP-01**, but you should open port 22 for both outbound and

inbound connections in your firewall.
Port 22 only needs to be opened for inbound connections. You must use SSH tunnel to connect to machine; tunnel to port 127.0.0.1:5900 for VNC protocol, and 127.0.0.1:80 for HTTP (web) control. OR, instead of SSH client, open ports 443 and 15900 (inbound) for HTTPS and encrypted VNC protocol. Then click always on the "encrypted" link. This is easier because you don't need to setup SSH tunnels.

## Appendix B Specifications

| | |
|---|---|
| Maximum supported video mode | 1600x1200 @ 85Hz |
| Standard video modes supported | 640x400 @ 85Hz<br>720x400 @ 85Hz<br>640x480 @ 60Hz<br>640x480 @ 72Hz<br>640x480 @ 75Hz<br>640x480 @ 85Hz<br>800x600 @ 56Hz<br>800x600 @ 60Hz<br>800x600 @ 72Hz<br>800x600 @ 75Hz<br>800x600 @ 85Hz<br>1024x768 @ 60Hz<br>1024x768 @ 70Hz<br>1024x768 @ 75Hz<br>1024x768 @ 85Hz<br>1152x864 @ 75Hz<br>1280x960 @ 60Hz<br>1280x960 @ 85Hz<br>1280x1024 @ 60Hz<br>1280x1024 @ 75Hz<br>1280x1024 @ 85Hz<br>1600x1200 @ 60Hz<br>1600x1200 @ 65Hz<br>1600x1200 @ 70Hz<br>1600x1200 @ 75Hz<br>1600x1200 @ 85Hz |
| Maximum power consumption | 18 watts |
| Dimensions WxDxH (mm) | 188 x 167 x 22 |
| Input Connectors | Video In Port (for the host computer)<br>Host Keyboard Port (PS/2, for the host computer)<br>Host Mouse Port(PS/2, for the host computer)<br>Video Out Port (for the local monitor)<br>Local Keyboard Port (PS/2, for the local keyboard)<br>Local Mouse Port (PS/2, for the local mouse)<br>USB Port ( 5-pin, mini-B)<br>LAN Port (RJ-45)<br>WAN Port (RJ-45)<br>R-Port (RJ-14)<br>DTE Serial Port (DB9 RS-232 Male)<br>DCE Serial Port (DB9 RS-232 Female)<br>DC in<br>DC in Spare |
| Regulatory Certifications | FCC Class A, CE |

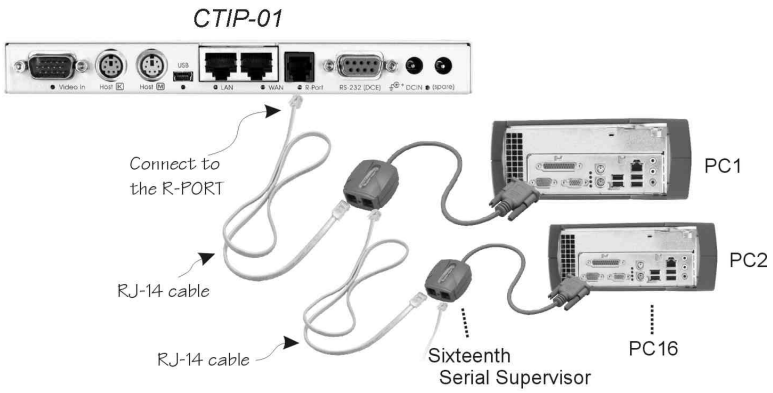
## Appendix C Supported Protocols

| Service | Description | Benefits |
|---|---|---|
| SSH | Secure Shell | May be used to securely “tunnel” VNC and HTTP protocols. |
| HTTP | Web redirector (to HTTPS) | Convenience server to redirect all web traffic to encrypted port. Clear-text HTTP is not supported. |
| SNMP | SNMP Agent (UDP) | Allows integration with existing SNMP network management systems. |
| HTTPS | SSLTLS Encrypted web control | Secure control and management of the device and attached system. Screen snapshots may be downloaded. Integrated Java VNC client (with or without encryption) allows control from any Java-enabled browser. Password protected. |
| VNC | VNC/RFB Protocol Server | Standardized real-time KVM network protocol. Compatible with existing VNC client software. |
| VNCS | SSL-tunneled VNC | VNC protocol tunneled via SSLTLS encryption. For secure real-time control of the server over public networks. |
| DHCP Dynamic IP Setup Config | | Eases network setup by locating IP address and other network settings from a centralized server. |
| RADIUS Centralized authentication | | Allows integration with existing RADIUS servers, so that user management can be centralized. Supports challenge-response authentication using hardware tokens (like SecurID) and conventional passwords. |
| SYSLOG | System event logging to another system | MIT-LCS UDP protocol. Must be configured via DHCP option. |
| DNS | Domain Name Service | Converts text name into IP Address Only used in the URL specification needed to emulate a CD-ROM. Use is optional. |

## Appendix D Using Optional Serial Supervisors (IPMI supported) with the R-Port of CTIP-01

**Background**

The **CTIP-01** offers a unique way to expand the functionality of the base product. Using R-Port on the rear panel of **CTIP-01**, you can add up to 16 **Serial Supervisors** serial devices using a specialized daisy-chain technology. The **CTIP-01** includes integrated control functionality that allows you to monitor and configure the devices with the RS-232 serial port using the interactive Web interface. To minimize space and infrastructure requirements, the **Serial Supervisor** uses a single cable to carry both the power and the data signal. All configuration settings are stored separately in ttached **Serial** in non-volatile that they will not be event of a power sconnection.



ıe cable. For the first **P-01**. Then, connect vo RJ-14 ports in the the first computer to ıg the second **Serial upervisor**) to link up 16 computers. The rding cabling, status **isor**.

**Configuring/Viewing Serial Supervisor through the Web Interface**

Once you have one or more **Serial Supervisors** connected, you will able to configure and manage them through the Web interface. You may need to modify the default settings on the **CTIP-01** to match your various **Serial Supervisors** default configuration. Consult the documentation that came with your **Serial Supervisor** to determine if you need to modify the default settings to complete the installation. To be able to configure your **Serial Supervisor**, you must be logged in as **admin**. Other users will be able to view which devices are active but cannot configure them.

Once you are logged in, choose the **Admin/Setup** option from the menu at the top of the Home screen in the Web interface. Click **External Serial consoles setup and control**. You will be presented with the **Serial Consoles Attached** menu, and a table with the following headings:

| # | Name / Description | Baud (bps) | Mode | Force DCD | Console Log | Connect... |
|---|---|---|---|---|---|---|

**#:** You can assign a value (**1** ~ **99**) to each attached serial device. This does not effect the configuration or operation of the device in any way, but is simply a means to sort this list for ease of management.

**Name/Description:** An identifier for the **Serial Supervisor** device. Like the number assignment, it is for ease of administration only.

**Baud (bps):** This is the communication speed for the device, and the setting here must match the setting on the device itself (see below). All common baud rates between 300 and 115,200 bps are supported.

**Mode:** Sets the character framing scheme that the **CTIP-01** will use with the **Serial Supervisor** device. You can choose from the following selections:

**8N1:** Eight bits, no parity, one stop bit (default and most common)
**7N1/701/7E1/7M1/7S1:** Seven bits, (none/odd/even/mark/space) parity, one stop bit
**8N1/801/8E1/8M1/8S1:** Eight bits, (none/odd/even/mark/space) parity, one stop bit
**8N2:** Eight bits, no parity, two stop bits

**Force DCD:** Forces the Carrier Detect signal to be active at all times. Normally, DCD becomes active when a new user connects and is dropped when the last user disconnects (a response that is similar to many modems). When active, the devices will logout and reset itself if the carrier signal is lost, increasing security. **NOTE** that this may not work with all devices and could impair proper operation in some circumstances. The default setting is off.

**Console Log:** Clicking this link will open a separate Web page that will display the last 200 characters committed to that device's console log. **NOTE** that existing data is overwritten automatically when the 200 character limit is reached.

(Optional, not shown) **IPMI:** This is an optional feature that requires the purchase of a software upgrade on the **CTIP-01**. Refer to Appendix D for more information about purchasing and using the IPMI upgrade. This feature will not appear on the menu if the upgrade is not installed.

You can make as many changes a needed on this menu at one time before applying your changes. Once you are satisfied with the changes you have made, click **Commit changes** to apply the new settings. Click **Refresh** at any time to see an updated list of attached **Serial Supervisor** devices.

**Advanced Configuration Using the Integrated SSH Shell**

In most cases, configuring the **CTIP-01** to the same settings as the **Serial Supervisor** devices you are connecting should allow the devices to work with a minimum amount of configuration. However, you can also change the default settings on each **Serial Supervisor** device to fit your preferences and the needs of your application.

If you click the **Connect…** button next to the device you want to configure, two new windows will appear. The smaller of the two is a login screen; the other is a SSH terminal window. Click the login window and sign in as **admin** (using the same password as the Web interface) to activate the terminal window. You will see a welcome banner similar to the following:

Baud rate: 115200 bps, 8N1
Connected to #1: (none)... (Press ***Ctrl*** + ***Shift*** + ***Space*** for menu).

You are now connected to the **Serial Supervisor** device. Commands you type will be echoed on the terminal screen. It offers a simple menu system that allows you to change its configuration settings. To access the menu press ***Ctrl*** + ***Shift*** + ***Space*** (underscore) on the keyboard to access the menu. It will be similar to the following:

RS-232 Menu (#1: (none), 115200 bps, 8N1)
Q – Disconnect

```
# - Send break
H – Hangup line (drop DCD)
E – Send Ctrl-Shift-_
L – Low log entries (line buffer)
1 – Show last 10 log entries
other – Return to connection
Press key ->
```

To execute the desired command, simply press the corresponding key on the keyboard. You can also execute the command and avoid the menu by pressing the ***Ctrl*** + ***Shift*** + ***Space*** key combination quickly and pressing the letter of the command. To quit the menu, press ***Q*** on the keyboard when the menu is active.

**Remote Login via SSH**

You can also use a standard SSH client to access the **Serial Supervisor** options if you wish to avoid using the Java-based SSH client in the Web interface. Simply use your SSH client (several freeware packages are available for download, along with commercial applications) and connect to the IP address of the **CTIP-01** using port 22 (default).

Login in to the SSH session as **admin** using the same password as the Web interface. At the command prompt type **connect x** (where **x** is the number of the **Serial Supervisor** device you wish to manage). Alternatively, you can enter the command **connect -l** to see a list of active devices.

**Operating NOTES**

- Hardware handshaking (CTS/RTS) is required for speeds exceeding 9600 bps. It is enabled by default on the **CTIP-01**, but may need to be enabled on the other end of the connection. For Unix systems, the command is:

  **stty –crtscts < /dev/[serial port]**
- **Serial Supervisor** devices use a simple RS-485 multidrop network running at 115,200 bps. It is possible that every **Serial Supervisor** device will not be inputting/outputting data at the same rate at all time. However, since these devices use interactive logins, it is unlikely that all channels would be busy at any one time. Hardware handshaking is used to limit the output rate of individual channels as needed.
- A maximum of four users may simultaneously login to the same device. All users may type commands at any time, and all users will see the same output. **NOTE** the following:
  a. All users have equal access to all channels.
  b. A maximum of 16 **Serial Supervisor** devices may be connected at any one time.

You plug-in and unplug any **Serial Supervisor** device at any time. When reconnected, it will automatically become available after a 15 second initialization period. Any log entries will be retained by the **Serial Supervisor** device while deactivated, but will not be available to users until it is re-initialized.

**IPMI (Intelligent Platform Management Interface) Function**

**Background**

To offer a more complete remote server control solution, the **CTIP-01** offers an optional power management feature that allows remote hardware restarts and the ability to power the host computer on and off. You may be able to take advantage of this feature if the host computer you are managing supports IPMI (Intelligent Platform Management Interface).

**Host Computer Requirements**

The host computer must support the IPMI standard version 1.5 to use this option. Most popular server motherboards now support the IPMI standard. To determine if your computer supports this IPMI, consult its

documentation for more information.
IPMI is used to configure and control a device on the motherboard called the BMC (Baseboard Management Controller) using a dedicated serial port. Once the computer is configured for IPMI management, the serial port on the host computer is normally reserved by the BIOS solely for that purpose and cannot be accessed or recognized by the operating system. It is therefore unlikely that a serial port provided by an add-in card will be able to act as an IPMI port, so you must use a serial port integrated on the motherboard of the managed computer. If the computer you are managing only has a single serial port, you must add an additional port (or ports) via an add-in card if you need a serial port for other purposes (i.e. modem). Enabling IPMI support usually requires enabling options in the host computer's BIOS setup software, and the instructions will vary considerably from make to make and model to model. Normally, a password will be created by the BIOS that allows the IPMI feature to be accessed; this password is exclusive to the IPMI feature and does not correspond to a password or account in the host computer's operating system.

**If the Host Computer Does Not Support IPMI**

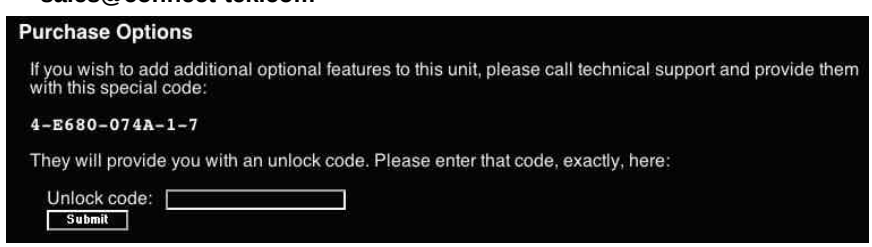
If the host computer you are managing with the **CTIP-01** does not support IPMI, **Connect-Tek** offers a non-IPMI solution that also works via serial port and acts as a power concentrator and a power management device: the 8 Outlet Serial Power Console and Switch. For more information about this product, visit **www.connect-tek.com**

**Activating the IPMI Option**

The **CTIP-01** contains the necessary software to use IPMI. To enable this capability, you must purchase the software option from **Connect-Tek** unless you have purchased a model with the feature pre-enabled. To verify whether the IPMI feature is enabled on your unit, login to the Web interface as **admin**, click the **Setup/Admin** button at the top of the page, and click **Firmware and flash memory management**. If **IPMI** is not listed beside **Software Options** (see above) then the IPMI option is not present and you will have to purchase the software option to use the feature.

To purchase the IPMI option, contact **Connect-Tek** Technical Support at:

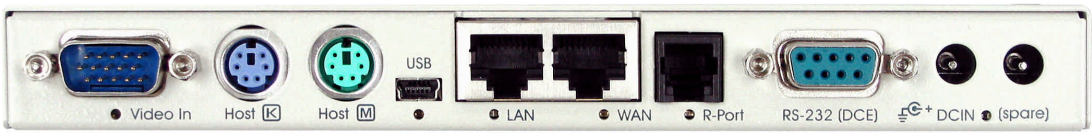
**sales@connect-tek.com**


Purchase Options
If you wish to add additional optional features to this unit, please call technical support and provide them with this special code:
4-E680-074A-1-7
They will provide you with an unlock code. Please enter that code, exactly, here:
Unlock code:
Submit

Have your model and serial number on hand. When asked, supply the technician with the code listed under **Purchase Options** at the bottom of the **Firmware and flash memory management** page. Once the order is processed, the technician will provide you with an Unlock code. Enter that code in the space provided, and click **Submit**. The system will update itself to allow IPMI configuration.

**Connecting the CTIP-01 for IPMI Control**

**Front Panel (DTE Serial Port)**




**Rear Panel (DCE Serial Port)**

You can use either serial port on the CTIP-01 to send IPMI access; your choice will dictate the type of cable you will use to make the connection. The DTE Serial port on the front panel requires the use of a null modem serial cable. The DCE Serial port on the rear panel requires the use of a straight through serial cable.

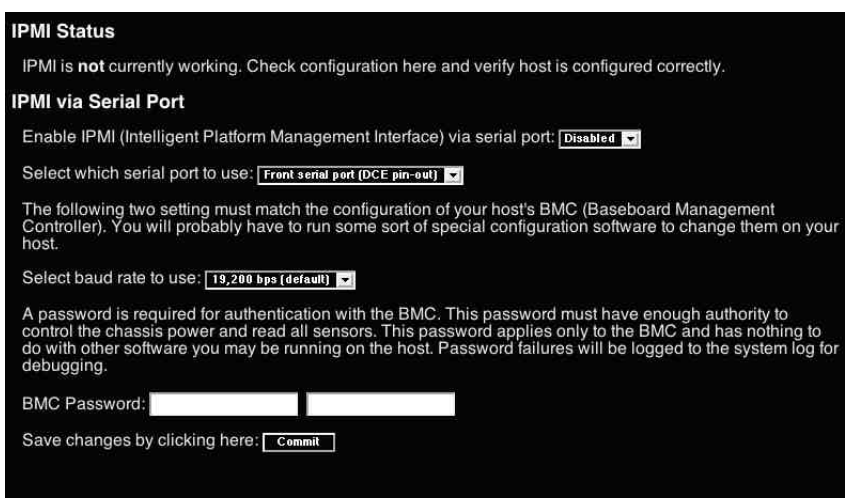
Connect a female end of a serial cable to the serial port that is configured for IPMI access on the host computer. Connect the opposite end (male if connecting to the **DCE Serial** port, female if connecting to the **DTE Serial** port) to the **CTIP-01**.

**Configuring IPMI on the CTIP-01**

Once you have connected the IPMI-configured serial port to the **CTIP-01** and enabled the software option, you can begin to configure IPMI settings through the Web interface.

**IPMI/IPMB** setup (Intelligent Platform Management)

Log in to the Web interface as **admin**. Click the **Admin/Setup** link at the top of the page and choose **IPMI/IPMB setup (Intelligent Platform Management)**.


IPMI Status
IPMI is not currently working. Check configuration here and verify host is configured correctly.
IPMI via Serial Port
Enable IPMI (Intelligent Platform Management Interface) via serial port: Disabled
Select which serial port to use: Front serial port (DCE pin-out)
The following two setting must match the configuration of your host's BMC (Baseboard Management Controller). You will probably have to run some sort of special configuration software to change them on your host.
Select baud rate to use: 19,200 bps (default)
A password is required for authentication with the BMC. This password must have enough authority to control the chassis power and read all sensors. This password applies only to the BMC and has nothing to do with other software you may be running on the host. Password failures will be logged to the system log for debugging.
BMC Password:
Save changes by clicking here: Commit

You will be presented with the **IPMI Status** menu (see above). Make the following changes to enable IPMI:

**Enable IPMI (Intelligent Platform Management Interface) via serial port:** select **Enabled.**

**Select which serial port to use:** select either **Front serial port (DTE pin out)** or **Rear serial port (DCE pin out)** based on how the **CTIP-01** is connected to the IPMI serial port on the host computer.

**Select baud rate to use:** select a value from the menu between **9600 bps** and **115,200 bps** based on the configuration on the host computer's IPMI settings.

**BMC Password:** Enter the password twice assigned to the BMC in the host computer's BIOS setup software.

**NOTE**: that the selected baud rate should match the host computer's setting. Problems with the BMC password (as well as any other error information) will be recorded in the **CTIP-01**'s system log on the **Status** page of the Web interface. If the host computer's BIOS setup allows for multiple levels of security for the BMC, ensure the password you enter on the menu offers sufficient authority to control chassis power and monitor fan status.

Once you have made the necessary changes on this screen, click **Commit** to activate IPMI with the settings you entered. **NOTE** that clicking **Commit** will cause any active VNC sessions to fail and you will need to re-establish them.

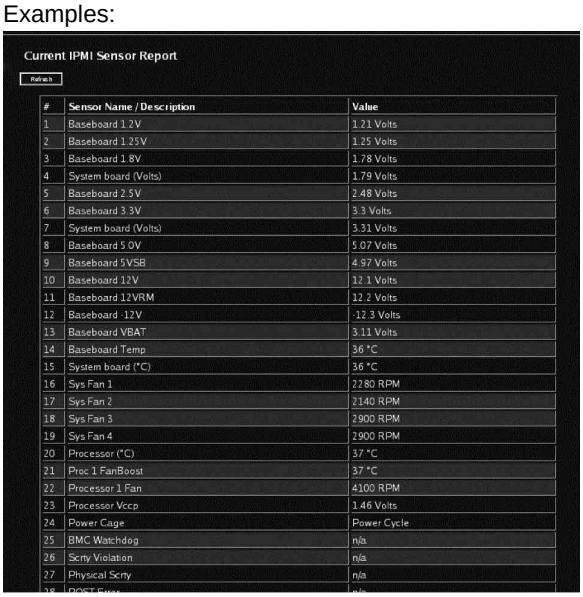
**Accessing the Status Screen**

The **CTIP-01** allows you to monitor the status of the host computer via IPMI using either the Web interface or the VNC client. The information you will be able to view using the status screen will depend on the model of host computer being managed. Since IPMI implementations vary widely across manufacturers, the information you are able to see on your status screen may differ from the examples. **NOTE** that the **Status** screen will not allow you to make any configuration changes and is for monitoring purposes only.

To access the **Status (IPMI Sensor Report)** screen:

- From the Web interface: click **View IMPI sensor report** next to the thumbnail image on the **Home** screen
- From the VNC interface: click **IMPI** from the Bribar at the bottom of the VNC window

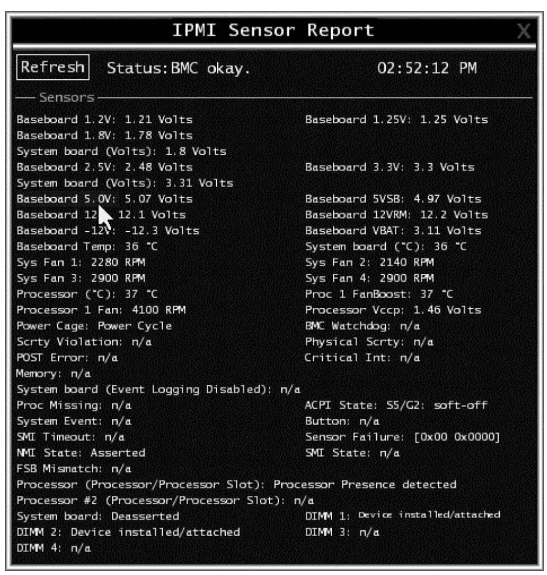
Examples:


Current IPMI Sensor Report

Refresh

| # | Sensor Name / Description | Value |
|---|---|---|
| 1 | Baseboard 1.2V | 1.21 Volts |
| 2 | Baseboard 1.25V | 1.25 Volts |
| 3 | Baseboard 1.8V | 1.78 Volts |
| 4 | System board (Volts) | 1.79 Volts |
| 5 | Baseboard 2.5V | 2.48 Volts |
| 6 | Baseboard 3.3V | 3.3 Volts |
| 7 | System board (Volts) | 3.31 Volts |
| 8 | Baseboard 5.0V | 5.07 Volts |
| 9 | Baseboard 5VSB | 4.97 Volts |
| 10 | Baseboard 12V | 12.1 Volts |
| 11 | Baseboard 12VRM | 12.2 Volts |
| 12 | Baseboard -12V | -12.3 Volts |
| 13 | Baseboard VBAT | 3.11 Volts |
| 14 | Baseboard Temp | 36 °C |
| 15 | System board (°C) | 36 °C |
| 16 | Sys Fan 1 | 2280 RPM |
| 17 | Sys Fan 2 | 2140 RPM |
| 18 | Sys Fan 3 | 2900 RPM |
| 19 | Sys Fan 4 | 2900 RPM |
| 20 | Processor (°C) | 37 °C |
| 21 | Proc 1 FanBoost | 37 °C |
| 22 | Processor 1 Fan | 4100 RPM |
| 23 | Processor Vccp | 1.46 Volts |
| 24 | Power Cage | Power Cycle |
| 25 | BMC Watchdog | n/a |
| 26 | Scrty Violation | n/a |
| 27 | Physical Scrty | n/a |

**Web Status Report**

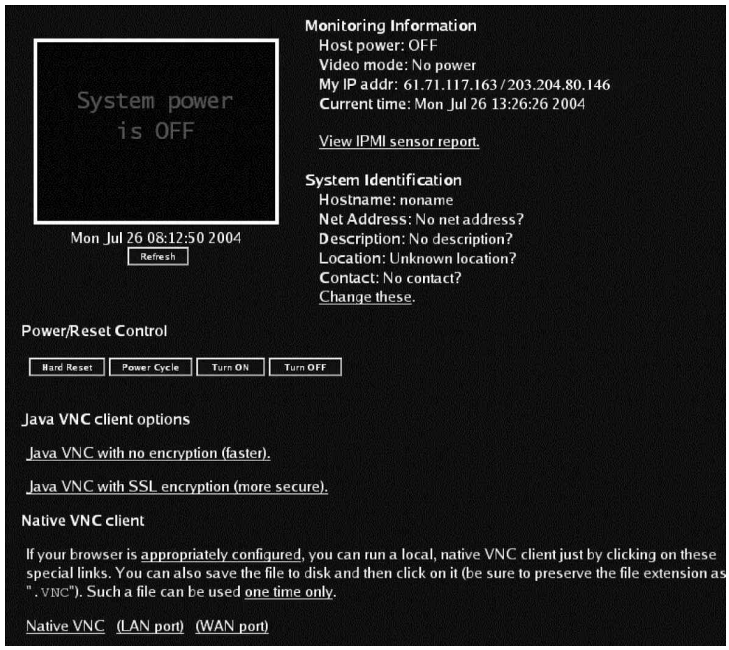



**VNC Status Report**

**Accessing IPMI Controls**

There are two ways to access power controls for the managed computer. The first is through the **Home** screen on the Web interface. The second is through the Bribar during an active VNC session.

**Web**


System power is OFF
Mon Jul 26 08:12:50 2004
Refresh
Monitoring Information
Host power: OFF
Video mode: No power
My IP addr: 61.71.117.163 / 203.204.80.146
Current time: Mon Jul 26 13:26:26 2004
View IPMI sensor report.
System Identification
Hostname: noname
Net Address: No net address?
Description: No description?
Location: Unknown location?
Contact: No contact?
Change these.
Power/Reset Control
Hard Reset
Power Cycle
Turn ON
Turn OFF
Java VNC client options
Java VNC with no encryption (faster).
Java VNC with SSL encryption (more secure).
Native VNC client
If your browser is appropriately configured, you can run a local, native VNC client just by clicking on these special links. You can also save the file to disk and then click on it (be sure to preserve the file extension as ".vnc"). Such a file can be used one time only.
Native VNC (LAN port) (WAN port)

**Controls on the Home Screen (Web)**

Once IPMI is enabled and functioning correctly, a set of controls will appear immediately under the thumbnail image of the host computer on the **Home** screen on the Web interface. **NOTE** that you must be logged in as **admin** to use this feature. From here, you have four options:

**Hard Reset:** Equivalent to pressing the RESET button on the managed computer. The computer will restart.

**Power Cycle:** The computer will power off, pause for a moment, and power on again automatically; equivalent to pressing the POWER button off and on again on the host computer.

**Turn ON:** Powers on the host computer.

**Turn OFF:** Powers off the host computer.

**VNC**

If you are inside an active VNC session and are logged in as **admin** you can use the Bribar to access IPMI features. You have two choices from the Bribar:

**Reset:** Equivalent to pressing the RESET button on the managed computer. (The computer will restart.)

**ON/OFF:** Powers the host computer on or off depending on the current state of the host computer; equivalent to pressing the POWER button on the host computer.

**NOTE:** IPMI may not automatically close the host computer software safely when you issue a reset or power off command. Since these features are equivalent to pressing hardware buttons on the computer itself, the computer will respond in exactly the same way. Always shut down your operating system and application software normally before issuing an IPMI command to avoid data loss or corruption.

# Appendix E Using Optional Modem Feature

**Background**

The modem option allows the **CTIP-01** to act as an Internet connection server for increased security and flexibility in connecting with the host computer. Unlike the TCP/IP connection used with the standard Web configuration and VNC clients, the modem creates a one-to-one connection between the **CTIP-01** and the computer you are using to manage the host computer that is essentially private, as it bypasses the public Internet completely. Note this option requires both an external modem (most standard connection protocols are supported) and a dedicated phone line that can be connected to the modem for external access. While it is technically possible to use the modem feature through some PBX systems, this increases the complexity and reduces the performance of the connection. For clarity, the instructions presented here assume that the modem is connected to a typical POTS (plain old telephone system) line that is not routed through a phone management system or shared with other devices. If you wish to use this feature through a PBX system, it may require some experimentation and additional support from your telecom services provider, and is not supported by Connect-Tek.

**Activating the Modem Option**

**A system without the modem option enabled**

The CTIP-01 contains the necessary hardware to attach a modem. To enable the modem capability, you must purchase the software option from Connect-Tek unless you have purchased a model with the feature pre-enabled. To verify whether the modem feature is enabled on your unit, login to the Web interface as **Admin**, click the **Setup/Admin** button at the top of the page, and click **Firmware and flash memory management**. If **MODEM** is not listed beside **Software Options** (see above) then the modem option is not present and you will have to purchase the software option to use the feature.

To purchase the modem option, contact **Connect-Tek** Technical Support:

**sales@connect-tek.com**

Purchase Options
If you wish to add additional optional features to this unit, please call technical support and provide them with this special code:
4-E680-074A-1-7
They will provide you with an unlock code. Please enter that code, exactly, here:
Unlock code:
Submit

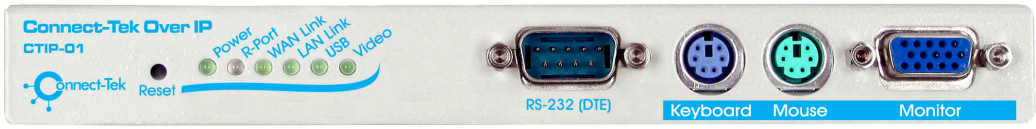
Have your model and serial number on hand. When asked, supply the technician with the code listed under **Purchase Options** at the bottom of the **Firmware and flash memory management** page. Once the order is processed, the technician will provide you with an Unlock code. Enter that code in the space provided, and click **Submit**. The system will update itself to allow modem configuration.

**Connecting a Modem**

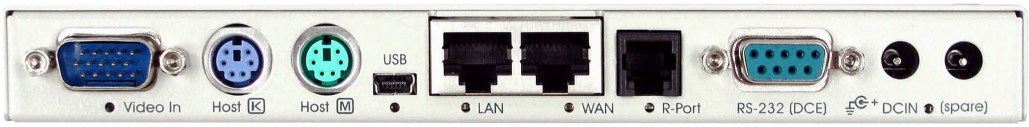
The **CTIP-01** will work with virtually any Hayes-compatible modem that recognizes the standard AT command set. Some modem manufacturers offer “enterprise” grade modem products (at a premium price) that include technology to improve the stability of connections; whether this type of product would be

beneficial to your application depends on whether you consider the modem connection to be mission-critical, the quality of your telecom infrastructure, and your budget for implementing this solution. The model of modem attached is essentially transparent to the **CTIP-01**.

It is important to note that modems that offer "56K" (or 56,000 bps) connections often achieve connection speeds that are far lower than their maximum capabilities. Given the limitations of telecom infrastructure (many locations have yet to implement fully digital switching technology, and still rely on older analog technology for some segments), the maximum "upstream" transfer rate is limited to a maximum of 33,600 bps between two modems; the "downstream" rate is often within a similar range for a typical connection. Therefore, speeds below 56,000 bps do not indicate a problem with the modem or the **CTIP-01** but simply reflect the line conditions at the time the connection is made.




**Front Panel (DTE Serial Port)**




**Rear Panel (DCE Serial Port)**

The **DTE Serial** port on the front panel can be used for serial port configuration when the modem is connected. It requires the use of a null modem serial cable.

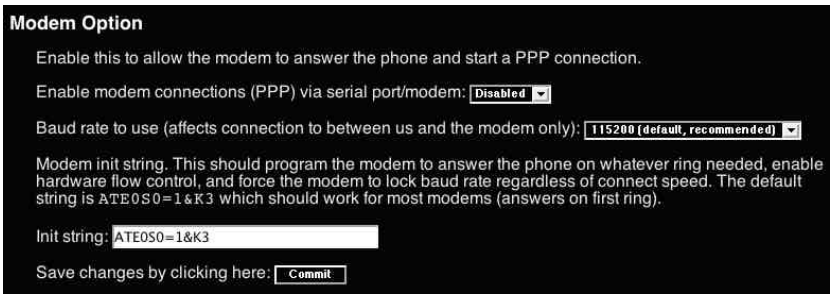
The **DCE Serial** port on the rear panel is used to connect the modem to the **CTIP-01** and requires the use of a straight through serial cable.

Place the modem near the **CTIP-01** and an available telephone jack. Connect the modem to the telephone jack, data cable, and power source according to the instructions in its documentation. The opposite end of the modem's data cable should be a DB9 female serial connection. Connect that end of the cable to the **DCE Serial** connection on the rear panel of the **CTIP-01**.

**Configuring a Modem Connection on the CTIP-01**

Most connections will work appropriately with the default settings on the **CTIP-01** once the feature is enabled. When you entered the Unlock code to enable the feature, the **CTIP-01** created a new menu option to enable configuration of this feature.

Login to the Web interface as **Admin**. Click **Admin/Setup** from the top of the page and choose **Modem (PPP) setup**.


Modem Option
Enable this to allow the modem to answer the phone and start a PPP connection.
Enable modem connections (PPP) via serial port/modem: Disabled
Baud rate to use (affects connection to between us and the modem only): 115200 (default, recommended)
Modem init string. This should program the modem to answer the phone on whatever ring needed, enable hardware flow control, and force the modem to lock baud rate regardless of connect speed. The default string is ATE0S0=1&K3 which should work for most modems (answers on first ring).
Init string: ATE0S0=1&K3
Save changes by clicking here: Commit

You will then be presented with the **Modem Option** menu (see above). Make the following changes to enable and configure the modem connection.

- **Enable modem connections (PPP) via serial port/modem:** select **Enabled**.
- **Baud rate to use (effects connection between us and the modem only):** select **115200**.
- **Init string:** leave as **ATE0S0=1&K3** (see below).

The baud rate dictates the connection speed between the **CTIP-01**'s serial port and the modem, and does not affect the connection speed between the local and remote modems, as they will negotiate their own connection speed when a connection is made. It is highly recommended that this setting be left at the default for best performance.

The init string is the command (using the standardized Hayes AT command set) that the **CTIP-01** will send to the modem to activate it. The string included should work with the majority of modems and configures the following connection properties: answer incoming calls on the first ring, enable hardware flow control, and lock the connection speed. Your modem's documentation will describe other potential init strings that you can use to alter the connection properties. For instance, you could commit the settings to the modem's non-volatile memory (NVRAM) or allow the modem to adjust the connection speed for greater stability (and so on). You may wish to test the connection with the default init string first before making changes specific to your modem model or situation to simplify the troubleshooting process.

Click the **Commit** button to save your changes and activate the modem feature with the specified settings.

**Configuring the Remote Connection**

This section describes how to configure a typical Windows dial-up session to access the modem connection on the **CTIP-01**. The instructions here relate to a **Windows XP** configuration; other versions of Windows are similar.

**Step 1**. Open **My Network Places** from the desktop or the **Start** menu.
**Step 2**. Click **View network connections**.
**Step 3**. Click **Create a new connection** under **Network Tasks**.
**Step 4**. The **New Connection Wizard** window will open. Click **Next**.
**Step 5**. Select **Connect to the Internet** and click **Next**.
**Step 6**. Select **Set up my connection manually** and click **Next**.
**Step 7**. Select **Connect using a dial-up modem** and click **Next**.
**Step 8**. In the space provided under **ISP Name**, type an appropriate name of your choosing for the connection. Click **Next**.
**Step 9**. In the space provided under **Phone Number** enter the phone number for the line to which the **CTIP-01**'s modem is connected. You may need to add the area code, country code, or other digits needed to access the outside line as appropriate. When finished, click **Next**.
**Step 10**. Make your choice from **Anyone's use** or **My use only** and click **Next**.
**Step 11**. Beside **User name** enter the user name of any valid user created using the Web interface of the **CTIP-01**. Beside **Password** and **Confirm password** enter the password that the user you entered above uses to access the Web interface.
**Step 12**. This screen also includes 3 checkboxes. **Uncheck all 3 checkboxes**.
**Step 13**. Click **Next**.
**Step 14**. You may select to add a shortcut to the desktop for this connection.
**Step 15**. Click **Finish**.

You can now use this connection to access the **CTIP-01** modem. Since you will still login to the unit through the Web interface after establishing a dial-up connection, the user name on the PPP connection and the user name used to access the Web interface do not have to be the same. For security purposes, you may wish to create a separate user name for dial-up access.

The unit will negotiate a PPP connection based on the settings you provided, and no additional scripting or configuration should be required under most circumstances. This is a summary of the settings for use with non-Windows operating systems, or other versions of Windows besides XP:

- PPP (Point-to-Point Protocol) must be used; no other authentication methods are supported.
- TCP/IP must be installed/enabled on the computer making the connection, and must be used for the dial-up connection.
- The connection must be configured to obtain a dynamic IP address.
- The user name/password must match a user currently configured on the **CTIP-01**.
- For best performance and to simplify the troubleshooting process, firewall software should not be used with the dial-up connection.

**Accessing the Web Interface**

Once a dial-up connection has been established, you can access the Web interface or start a VNC session using the following IP address:

**https://99.99.99.99**

You can now login to the Web interface (and/or VNC session) normally. Note that the remote machine (the one you dialed from) is automatically assigned the IP address 99.99.99.100 for the PPP session. This, and the IP address of the **CTIP-01**, cannot be modified. The following TCP/IP port numbers are assigned for a PPP connection, regardless of the settings configured in the Web interface for the **LAN** or **WAN** ports:

HTTPS: 443
VNC (clear-text): 5900
VNC (SSL secured): 15900
SSH: 22

**Performance Notes**

All images over the PPP connection will be grayscale to conserve bandwidth. If other users are connected while a PPP session is active, their screens will be in grayscale as well. When PPP is inactive, color is automatically re-enabled.

Some areas of the screen may not be updated as frequently as others, and animations or other auto-updating areas of the screen may appear out-of-focus or “blocky” as a result. Since the area around the mouse pointer is refreshed most frequently, hold the pointer over an area to improve its clarity.

It may be beneficial to minimize any unnecessary icons, backgrounds, or other clutter on the host computer’s desktop to make the dial-up connection as efficient as possible.

When the modem feature is enabled, you can use a “line modem” connection on the serial port using a serial cable to begin a PPP session. If you are using the **DTE Serial** port on the front panel, use a null modem serial cable. If you have disconnected the modem and are using the **DCE Serial** port on the rear panel for the PPP connection, use a straight through serial cable. When the modem is not actively connected, you can begin a PPP session at up to 460 kbps. To hang up and re-connect the modem, end the PPP session.

If you need to configure the device over a serial connection while the modem option is enabled, connect a serial cable (see immediately above for instructions on what type of cable to use for the port you are accessing on the **CTIP-01**) and begin a terminal session following the instructions under “Terminal Configuration Using a Serial Cable” in this manual. Once connected, you will see the following message:

**Expecting a modem, if human, type admin password (Or start PPP)**

Type the password for user **admin** and press enter. The password will not appear on the screen. The configuration menu will appear. Make the changes you wish or press **q** and **Enter** to exit and leave the modem connection active.

**Troubleshooting Guide**

The following messages will appear in the system log on the **Status** screen in the Web interface and may help to diagnose problems with the modem configuration.

**Starting PPP (for auth) on port…**

Modem is connecting and the PPP login process is starting.

**Modem hang up. Resetting**
The connection has been closed or terminated unexpectedly.

**Timeout during login process. Giving up**
The PPP client connecting over the modem has waited too long to complete the authentication process or supplied an invalid user name and/or password.

**Modem init chat script failed**
The modem did not respond to the initialization string from the CTIP-01. You may need to change the init string or verify the cabling and modem status.

**Modem init okay**
The modem has responded appropriately to the init string.

**Saw PPP startup from client**
A PPP authentication has occurred and a session has started.

**Phone line rings!**
An incoming call has been detected by the modem.

**Modem answers: xxxxxxxxx**
The connection speed and protocol used for a connection, as reported by the modem. The exact contents of the message will vary depending on the modem make and model.

## Appendix F The Installation of Optional CTIP-01 Rack Mounting Bracket: RACKMT-IP

A special bracket is available for the rack-mounting **CTIP-01**. It allows rack mounting in two different orientations ---horizontally and vertically as shown as Figure 1 and Figure 2 respectively. There is also a rack-shelf available that mounts two **CTIP-01** systems into 1U of space.

**Note: If you would like to install one CTIP-01 horizontally on the rack, 2 brackets are necessary, please refer to Figure 1 as well.**

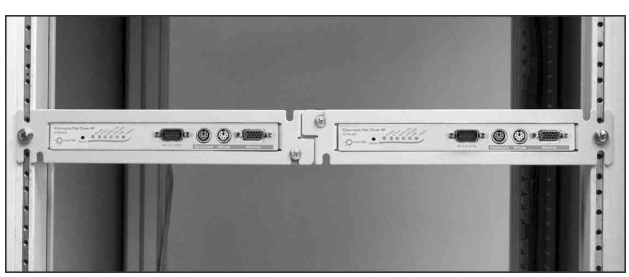


Figure 1

Figure 2

# Limited Warranty

Connect-tek, Inc., hereby warrants that this product shall be free from defects in materials and workmanship for a period of one (1) year, from the date of delivery to the original purchaser. Connect-Tek's sole responsibility with respect to this warranty shall be to repair or to replace at Connect-Tek's option, any product or part thereof determined by Connect-Tek to be defective. Connect-Tek expressly states that this warranty does not include this product's compatibility with any specific computer make or model, operating system or application.

This warranty is not extended to include accessories.
To enforce this warranty, contact your place of purchase and your representative will provide the required authorization. CONNECT-TEK EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, EXCEPT AS THOSE SPECIFIED HEREIN.

LIMITATION OF LIABILITY

CONNECT-TEK'S LIABILITY, IF ANY, FOR DAMAGES RELATING TO THIS PRODUCT, REGARDLESS OF THE NATURE OF THE ACTION BROUGHT, IS LIMITED TO THE ACTUAL PRICE PAID BY THE PURCHASER FOR THIS PRODUCT, AND WILL, IN NO EVENT INCLUDE ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL OR OTHER DAMAGES OF ANY KIND, EVEN IF CONNECT-TEK HAS BEEN APPRISED OF THE LIKELIHOOD OF SUCH OCCURRING, OR IF SUCH DAMAGES WERE REASONABLY FORESEEABLE.

EXCLUSION OF WARRANTY

THIS WARRANTY DOES NOT COVER ACCIDENT, MISUSE, FIRE, FLOOD, AND ANY OTHER ACT OF GOD, INCORRECT LINE VOLTAGE, DAMAGE CAUSED BY IMPROPER INSTALLATION, IMPROPER OR UNAUTHORIZED REPAIR OR MARRED CABINET, MISSING OR ALTERED SERIAL NUMBERS, AND CUSTOMER ADJUSTMENTS THAT ARE NOT COVERED IN THE INSTRUCTION MANUAL.

Connect-Tek, Inc. makes no representation or warranties with respect to the contents of this manual and disclaims any implied warranties for fitness for any particular application. Connect-Tek, Inc., reserves the right to revise this manual without obligation to notify any person or organization of such revision.

All rights reserved. Reproduction of any part of this manual in any form whatsoever without Connect-Tek's expressed written permission is prohibited.
Copyright 2005 by Connect-Tek, Inc.

The brand and product names mentioned in this manual are trademarks of the manufacturers and publishers and are used only for the purpose of identification.

PP5-NH0000-009
Printed in Taiwan